This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

RAND EUROPE

Cyber-security threat characterisation

A rapid comparative analysis

Neil Robinson, Luke Gribbon, Veronika Horvath, Kate Robertson

Prepared for the Center for Asymmetric Threat Studies (CATS),
Swedish National Defence College, Stockholm

The research described in this document was prepared for the Center for Asymmetric Threat Studies (CATS), Swedish National Defence College, Stockholm.

Published 2013 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
RAND URL: http://www.rand.org
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

Based on an assignment from the Swedish Cabinet Office and Department of Defence, the National Defence College's Center for Asymmetric Threat Studies (CATS) in Stockholm asked RAND Europe to undertake a rapid comparison of states' characterisation of cyber-security threats. This involved investigating three lines of enquiry related to the integration of cyber-security within broader national and transnational defence and security frameworks.

The project was limited both in size and scope and called primarily for desk research. This document is the final deliverable for this study, encompassing results and analysis from desk research, and insights gleaned from previous research on the issue.

The first part of the document summarises the findings and provides an overview of the scope and methodology of the research. The second part of the document describes the cyber-security strategies and approaches in ten case studies: Canada, Denmark, Estonia, Finland, France, Germany, Netherlands, Russian Federation, the UK and the USA. At CATS' request we also have profiled initiatives by NATO and the EU. Based on documentary analysis, stakeholder engagement and previous studies, we include a short chapter on potential policy concerns for Sweden going forward, supplementing the case study analysis. The report will be of interest to practitioners and policymakers in cyber-strategy and policy.

RAND Europe is an independent, not-for-profit policy research organisation that aims to improve policy and decision making in the public interest, through research and analysis. RAND Europe's clients include European governments, institutions, non-governmental organisations and firms with a need for rigorous, independent, multidisciplinary analysis.

We would like to thank our Quality Assurance reviewers Charlie Edwards and Dr Emma Disley for their helpful and insightful comments in the preparation of this report. For more information about RAND Europe or this project, please contact:

Neil Robinson
Research Leader, Defence and Security
RAND Europe
Westbrook Centre, Milton Road
Cambridge CB4 1YG, United Kingdom
Tel. +44 (1223) 353 329
Email: neilr@rand.org
Web: www.randeurope.org/cyber

Contents

Executive summary

The Swedish National Defence College and its Center for Asymmetric Threat Studies (CATS) asked RAND Europe to undertake a rapid comparison of developed states' characterisation of cyber-security threats. This involved investigating three axes of analysis related to the integration of cyber-security within these states' broader national security and defence frameworks. The aim of this descriptive study was to act as an additional perspective and challenge to the activity underway to develop a cyber-security strategy in Sweden.

- **How are cyber threats prioritised and related to other national-level security issues across developed states?** For example, in the UK, cyber is one of the highest tier of threats within the Strategic Defence and Security Review 2010, with an allocated, defined cyber-security programme over four years, totalling £650m.[1]
- **What are the specific types of threat characterised within the cyber-security threat picture?** For example, the typology of threat actors; their strategic intent, motivation and tactical capabilities; how they have developed and responded to counter-measures; how states such as China and Russia frame their cyber-security and defence policies.
- **Who or what organisations have the policy lead in terms of roles, responsibilities and agencies' scope? What role do law enforcement agencies play, and where do they fit in this context?**

The project was limited both in size and scope and called primarily for desk research. Below, the high-level findings are summarised relating to the three questions investigated in this rapid comparative study. An overall message is that ostensible similarities in countries' cyber-security policy aims must be probed, as the research presented here suggests that they can mask differences in definitions, approaches and resultant programmes of action.

[1] UK Cabinet Office (2011).

Findings

Table E.1. Overview of the findings for the three questions

Comparator	Level of prioritisation	Characterisation of threat	Lead responding authority
Canada	One of seven highest	States (military and espionage) Cybercriminals Terrorist groups	Coordinating team within Public Safety Canada
Denmark	Highly likely	Financial damage Disruption or control of IT infrastructure and electronic warfare Espionage Cyber-relevance of terrorist threats	Sector responsibility, but leadership through the Danish Security and Intelligence Service and the National High Tech Crime Centre
Estonia	High (4 on a 5x5 matrix of impact and likelihood)	Focus on effects of threat actors	Estonian Authority for Information Systems
Finland	–	No typology available	Distributed among government departments
France	Major threat	No typology publicly used	Prime ministerial-level organisation (Agence Nationale de la Sécurité des Systems d'Information, ANSSI)
Germany	–	Terrorism, crime and war; natural hazards and technical failure or human error	Federal Ministry of the Interior and National Cyber Defence Centre (NCAZ)
The Netherlands	High priority	States Private organisations Professional criminals Terrorists Hacktivists Script kiddies Cyber-researchers Internal actors Non-actor	National Cyber Security Centre
Russian Federation	Most prominent	Internal (crime and corruption) External (state, terrorists, foreign competition)	Security Council of the Federation/Ministry of Defence National system of information protection and intelligence community
UK	Tier 1 (highest level)	Criminals Nation-states Patriotic hackers Terrorist groups Hacktivists	Cabinet Office level entity: Office for Cyber Security and Information Assurance
USA	Priority (one of four)	Criminal hackers Organised criminal groups Terrorist networks Advanced nation	Distributed across a number of organisations with inter-agency policy committee

		states	
NATO	Priority challenge (alongside four others)	None publicly available	Cyber Defence Management Board Cyber Defence Management Agency NATO's Computer Incident Response Capability
EU	–	None publicly available	Separate institutional mandates across protection of infrastructure of the EU (Computer Emergency Response Team, CERT-EU) Policy to tackle cyber-crime (DG HOME/Europol) International security and defence (European External Action Service/European Defence Agency) and business/government security (Directorate-General for Communications Networks, Content and Technology [DG CNCT]/European Network and Information Security Agency [ENISA])

Threat prioritization and relationship to other threats

For all countries examined where information was available, cyber-security threat had been prioritised highly in the top tier of security issues in national risk assessments in the last five years. However, higher prioritisation of threat has not consistently translated into greater resource allocated to the area: France, Germany, the UK and the USA have emphasised the importance of cyber-security and allocated significant cyber-specific funding streams. Others such as the Netherlands have prioritised cyber-security without making formal commitments to enhancing funding.[2] For other countries, given that cyber-security's definition in policy documents ranges from the protection of infrastructure to protection of the information society, it is highly likely that policy approaches and prioritisation will be different across states.

The findings from the case study countries provide examples of governments relating cyber threats to other areas. For example, Canada, the Netherlands and the UK have noted the migration of foreign state espionage to the cyber-environment, and are investing in responses. Moreover, in terms of impact we have identified instances where governments

[2] We were unable to obtain information for Denmark, Finland and Russia regarding spending totals, and we exclude the North Atlantic Treaty Organization (NATO) and the European Union from this part of the analysis.

are aware of the interdependencies between critical national infrastructures (eg France and the UK) and the cascade effect resulting from, for example, a cyber-attack during a natural disaster (eg Canada).

Characterisation of threat actors

With the exception of Russia, countries generally recognise a common set of threat actors, but the sophistication of the typologies of these actors vary by state. Some states such as the Netherlands have provided fuller characterisations of threat actors' motivations and targets. Additionally, countries place different emphasis on the capability and intent of these actors.

Our analysis of the development of cyber-security strategies gained from a document review suggests that cyber-security strategies are responsive to events, and hence over the last five years the emphasis has changed from a focus on transnational, terrorist threat actors to a framing of cyber-security in terms of defence and increasingly offensive capabilities against cybercriminals, state actors and their proxies. Key events which have both prompted governments to produce strategies and shaped their content include:

- the distributed denial of service (DDoS) attacks against Estonia in 2007;
- growing concern over China's digital espionage capability;
- serious and organised criminals' publicised attacks against business intellectual property;
- high-volume, low-level internet-enabled fraud; and
- the continued and intensive targeting of financial systems and governmental protectively marked information.

Governments will continue to be responsive in characterising threats; however, there is little evidence from the available literature that they have established systematic ways to forecast what future threat actors may appear on the cyber-scene.

Cyber-security leadership and the role of law enforcement authorities

Almost all of the case study countries have opted for an inter-departmental model of response to cyber-security, maintaining existing 'real world' remits in the cyberworld: for example, police managing cybercrime investigations, and security services tackling espionage. Policy leadership is commonly allocated to a coordinating body to bring together departmental responses and ensure deconfliction. In some instances these are 'new' coordinating bodies (eg Estonia and France); in others they are bolted on to existing governmental departments (UK and Canada). Overall, there is little consistency in the department assigned this role across the comparators. The body in charge of leading or coordinating policy varies from cabinet offices to interior ministries, and defence or national security directorates. There may be implications in terms of international cooperation due to this unevenness and mismatch in leadership bodies. We suggest that mapping in detail the 'hubs' of institutional cyber policy decision-making in each country would be a valuable research exercise, in order to give insight into international cooperation on cyber.

The scope of law enforcement's competences are different across states. Some have units with more developed cyber-security functions (eg France and the UK), whereas others such as Russia appear to place less emphasis on the role of mainstream policing in tackling cybercrime. Uneven consideration is given between countries to the role of computer emergency response teams (CERTs) in national response.

Going forward

The Swedish government is in the early stages of preparing to formulate its cyber-security strategy, so this report is unable to make further determinations on recommendations, other than to indicate the following:

- Use international comparisons carefully – care should be taken when leveraging practice from elsewhere, as the underlying context will be different. The Swedish government should frame how it learns from other states from the perspective of its own priorities.
- Distinguish between risk and threat – in order to properly inform responses, care needs to be taken to identify threats as threats (ie types of actor that might act strategically) and not risks (which include judgements on vulnerability and impact).
- Consider multidisciplinary approaches to threat assessment and prioritisation – an approach which uses different methods (qualitative and quantitative) could offer a more robust perspective than one that is based on single, more subjective analysis.

CHAPTER 1. Research outline

1.1 Research question

Based on an assignment from the Swedish Cabinet Office and Department of Defence, the National Defence College's Center for Asymmetric Threat Studies (CATS) in Stockholm asked RAND Europe to undertake a rapid comparative exercise, investigating three lines of enquiry related to the integration of cyber-security within broader national security and defence frameworks. These lines of enquiry were as follows.

- **How are cyber threats prioritised and related to other national-level security issues across developed states?** For example, in the UK, cyber is the highest priority of threat within the Strategic Defence and Security Review 2010, with an allocated, defined cyber-security programme over four years, totalling £650m.[3]
- **What are the specific types of threat characterised within the cyber-security threat picture?** For example, the typology of threat actors; their strategic intent, motivation and tactical capabilities; how they have developed and responded to counter-measures; how states such as China and Russia frame their cyber-security and defence policies.
- **Who or what organisations have the policy lead in terms of roles, responsibilities and agencies' scope? What role do law enforcement agencies play, and where do they fit in this context?**

1.2 Research aim

This report seeks to inform CATS as to how ten selected states characterise cyber threats: that is, a current profile of those states' cyber-security posture. This in effect involves an investigation of national frameworks to address threats and their portrayal of the actors involved in both threat and response.

Expert consensus suggests that one indicator of a country's cyber-security development is to have published strategies and action plans relating to cyber-security.[4] Thus, we have treated these documents (where available) as important in understanding the cyber-security profile and posture of the ten case study countries. Additionally, we have used open-source

[3] UK Cabinet Office (2011).

[4] *The Economist* Intelligence Unit and Booz Allen Hamilton (2012).

national risk assessments, which use 'all hazards' methodologies as a further source of information. In addition, we have profiled the cyber-security positions of the European Union (EU) and North Atlantic Treaty Organization (NATO).

This chapter provides an outline of the research that RAND Europe was asked to perform. The following chapters consider key terms in the field (Chapter 2), and undertake a case study analysis of ten states' cyber-security profiles and initiatives at the NATO and EU level (Chapter 3). This report then cross-references information from the case studies against insights into these topics derived from other research and our general domain knowledge on the cyber-security policy context in a report from a roundtable meeting held in Sweden to present interim findings (Chapter 4). A synthesis of the conclusions is then provided (Chapter 5).Drawing on the documentary analysis and stakeholder insights, some forward looking policy themes are outlined (Chapter 6) which are pertinent to Sweden, noting that Sweden is in the early stages of developing a cyber-security strategy.

1.3 Selection of case study countries

The case studies were selected by RAND Europe after a discussion with CATS. The research focused on ten states which fulfilled at least one of the following criteria:

1. States with advanced cyber-security responses or strategies which are considered to be sophisticated.[5] The strategies of these states may have recently undergone review, and are regarded by experts in the field as 'state of the art' (Canada, France, Germany, the Netherlands, the UK and the USA);[6]
2. States within Sweden's Nordic or Baltic neighbourhood that have similar strategic concerns, and may face a comparable range of threat actors (Denmark, Estonia and Finland – these three are a subset of criteria 1 states);
3. States which are viewed as ambiguous players in cyberspace, and are considered by some Western states to be potential strategic adversaries (Russia).[7]

Additionally, CATS requested that the EU and NATO be included within the analysis.

[5] The Cyber Power Index takes the existence of national cyber-security strategies as an indicator of 'cyber power' and assesses countries' strategy's level of sophistication. See: http://www.cyberhub.com/CyberPowerIndex

[6] European Network and Information Security Agency (ENISA) (2012a).

[7] United States Government Office of the National Counterintelligence Executive (2011).

The country comparators examined are listed alphabetically in Table 1.

Table 1: List of case studies

Countries and Intergovernmental Institutions		
Canada	France	UK
Denmark	Germany	USA
Estonia	Netherlands	*EU**
Finland	Russian Federation	*NATO**

*Supranational or regional entities

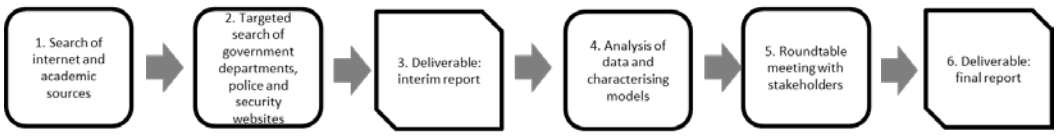
1.4 Definition of cyber-security threats

It is not within the scope of this comparative analysis to be prescriptive as to the nature of cyber-security threats. This is partly because, as experts reviewing only a subset of EU Member States' strategies have noted, "there is little consensus on the nature of threat and where emphasis should be placed".[8] Acknowledging that there is little consensus as to what constitutes a cyber-security threat, for the purposes of this analysis we include all threats outlined within the cyber-security strategies or wider policy documents of the ten case study countries. Definitional issues regarding cyber-security threats are discussed in Chapter 2.

1.5 Research methods

Information was gathered through desk-based research. The case study method uses publicly available secondary literature, news articles and documents containing information relevant to the three research questions set out above. The overall approach has four stages of analysis and two deliverables, and is illustrated in Figure 1.

Figure 1: Overview of approach



The first stage was a search of the internet and Google Scholar using search terms related to cyber threats and governmental cyber-security response,[9] supplemented by documents known to the study team from previous research. This search yielded 70 relevant documents from which information relevant to the research questions was extracted. The second stage involved a targeted review of websites of selected jurisdictions' governments, security agencies, police forces and security councils, in order to identify and extract information relevant to the three lines of enquiry. Researchers with relevant languages

[8] Luiijf et al. (2011).

[9] Search terms used were: (cyber-threats OR cyber strategy OR cyber-defence OR cyber-security) AND [country name].

were used to assist in reviewing websites. The deliverable resulting from analysis of this information was an interim report outlining the early findings from the desk research. The fourth stage involved analysis of the information extracted from the sources identified in the above stages and grey literature, in order to characterise the cyber-security posture of each of the ten case study countries. These characterisations were validated during a roundtable with representatives of CATS.

1.5.1 Quality of information identified

Academic literature yielded little comparative analysis of the way in which threats are prioritised, or of departments and agencies' roles in cyber-threat analysis. Grey literature provided descriptions of the cyber threats which states had encountered, and some limited information about how states had changed their cyber-security regimes in response to threats. National government and police websites provided more detailed (but necessarily open-source) descriptions of the way in which cyber-security was organised, as well as the strategic plans in place in the country.

There was significant variation in the quantity and quality of information available about each case study country. Information on Western European and North American countries was more readily available than that for Russia. In the case of the EU and Finland, there was less public information to review as their cyber-security strategies are in development. Relevant information on Russia was the hardest to obtain, potentially due to its more ambivalent position on cyber-security.

Given the nature of this as a rapid comparative exercise, the research represents a snapshot in time – describing the situation as at October 2012 – and is based upon information contained in the open-source documents reviewed.

It was beyond the scope of this report to undertake in-depth validation of information contained in the sources identified. Data are clearly sourced and presented with caveats where appropriate.

CHAPTER 2. Defining terms

This chapter will summarise three elements which are important to consider when characterising a country's cyber strategy:

1. the nature of national-level cyber threats;
2. the sources and/or actors from which they emanate; and
3. a consideration of the array of national-level actors and/or means required to address threats and vulnerabilities.[10]

2.1 Definition of threats

Cyber threats to states may be defined as those actors or adversaries exhibiting the strategic behaviour and capability to exploit cyberspace in order to harm life, information, operations, the environment and/or property. The cyber threat landscape is not necessarily revolutionary.[11] The activities that actors posing a threat can undertake are the same as those in the real world: crime, intelligence gathering and espionage, ideological activism and 'warfare'. These threats emanate from a range of sources: from disgruntled insiders to organised crime, identity thieves and terrorist or activist groups to hostile states and their proxies.[12] Nation-state reliance upon cyberspace means that this domain has become an increasingly attractive target for various types of adversary.[13]

Notable incidents of cyber threats in Sweden or in the Nordic and Baltic geopolitical neighbourhood illustrate the diversity of threats. These have attracted attention for their potential to inflict costs and damage states and their citizens' lives, information and property. Domestically, Sweden has suffered significant breaches of personal data from the users of a prominent blog, Blogtoppen. These breaches inflicted significant loss of Swedish

[10] These three elements are also part of the wider concept of risk assessment; however, risk assessment is excluded from this study as an appreciation of impacts or consequences would need to be considered. This is out of scope, as CATS is specifically interested in the context and drivers of threats (i.e. motivated strategic adversaries).

[11] Anderson et al. (2012).

[12] Khalizad et al. (1999).

[13] Khalizad et al. (1999).

users' personal information in October 2011.[14] Most recently, official Swedish government systems were hit by distributed denial of service attacks in early September 2012.[15]

In Sweden's region, states such as Estonia have been subject to cyber-attacks which experts have attributed to adversaries motivated by political grievance and power politics.[16] Annex A provides some examples of cyber-security incidents which have affected developed states since 2009. The attack against Estonia and the sectors targeted within the cyber-security incident table (Annex A) suggest that Sweden's government and defence sector, as well as high-technology, energy and telecoms industries, would be likely targets of hostile foreign state actors motivated by economic reasons and technology transfer.

Given the breadth of these threats, a typology of actors is helpful. Table 2 offers a high-level typology of actors posing threats in cyberspace, and an outline of their aims.

Table 2: Threat actor typology

Type	Sub-type	Goal
Individuals	Grey hats	Mayhem, joyride, minor vandalism
	Black hat	
Coordinated sub- or pan-national groups or networks	Criminal groups	Money, power
	Terrorists (political)	Gaining support for and deterring opposition to a cause
	Hacktivist (anarchistic/millennial)	Protest, fear, pain, disruption
	Insurgent groups	Overthrow of a government or separation of a province
	Commercial organisation	Industrial espionage, sale of information
States	Rogue state	Deterring, defeating or raising the cost of a state's involvement in regional dispute
	Peer competitor	Deterring or deferring a country in a major confrontation, espionage, economic advantage

Source: Adapted from Khalilzad (1998)

This typology, developed in 1998 (some 14 years ago) has stood the test of time and, when set alongside other threat models used nationally, remains relevant.

2.2 Actors: national-level stakeholders in cyber-security

Deterring and countering these types of threat and maintaining security in cyberspace involves a number of actors spread across the public and private sectors, as well as society as a whole. Examples of the breadth of actors involved in response include:[17]

- national-level policy units with responsibility for cyber-security issues – for example, the Office of Cyber Security and Information Assurance (OCSIA) in the UK, and Estonian Authority for Information Systems (RIA) in Estonia;

[14] Khalizad et al. (1999).

[15] Al Jazeera (2012).

[16] Traynor (2007).

[17] Robinson et al. (2012).

- national-level coordinating units or institutions with responsibility for critical national infrastructure protection missions – eg Centre for the Protection of National Infrastructure in the UK, and National Infrastructure Coordinating Center in the Netherlands;
- specific inter-governmental units dedicated to national cyber-defence missions – for example, the Cyber Security Operations Centre in the UK;
- operational agencies – intelligence, armed forces and law enforcement authorities – agencies which may be involved in the delivery of elements of the state's cyber capability: cyber deterrence, cyber-warfare, investigation, countering or investigating cybercrime, for example USCYBERCOM and the National Security Agency in the USA;
- national and/or governmental computer emergency response teams (CERTs) – types of CERT which collate and receive information from other CERTs with whom they have a peer relationship, but have a specific role to play in protection of the critical information infrastructure;
- communication service providers responsible in varying ways for parts of the infrastructure which make up 'cyberspace' – they may include 'essential' providers, which provide backbone, long-haul interconnectivity to mobile network operators or retail internet service providers. Some forms of provider may even be 'virtual' – resellers of bandwidth or access to different markets (for example, BT and C&W in the UK, Verizon in the USA);
- infrastructure hardware providers such as Cisco, Juniper Networks or Huawei – these companies manufacture the hardware and middleware and provide software for the infrastructure. Some such companies also have a systems integration role, which can have security implications when the nationality of the company (eg Huawei) may not be a close ally, or essential intellectual property for critical national infrastructure is unobtainable (US companies);
- software and services providers which design, develop, produce and market software – such firms may specialise, for example, in cryptographic software, infrastructure or services, and other industry firms including those in the integrated semi-conductor industry which design microchips (eg ARM or Intel).

As illustrated in Table 2, there is considerable divergence between the case study countries as to which part of government is assigned responsibility for leading cyber-security policy.

Table 2: Examples of organisations taking the lead in policy response

Policy lead department	Countries
Cabinet offices	UK: OCSIA
Specialised agency	Estonia: RIA; France: Agence Nationale de la Sécurité des Systems d'Information (ANSSI)
Ministry of Finance	Finland
Ministry of Interior	Canada: Public Safety Canada Germany: Federal Ministry of Interior (BMI)
Defence/Intelligence	Russia: Security Council of the Federation Denmark: Intelligence Service

Prime minister or president	France: ANSSI answers to the prime minister USA: efforts to create a White House cybersecurity coordinator through Executive Order of 2012

This chapter has introduced the concepts of cyber-security threats and provided some background as to where responsibility might lie within government for ensuring cyber-security. The next chapter sets out information on these elements for each of the ten case study countries and the two supranational entities.

CHAPTER 3. Comparators

This chapter presents data on ten national comparators (ordered alphabetically), and then two supranational institutions according to a standardised framework. Each comparator section begins by summarising how the comparator answers the three research questions. The chapter then provides a short policy background illustrating recent developments of note, and goes on to detail each of the aspects of the research question in turn. A conclusion section synthesises this chapter.

3.1 Canada

3.1.1 Summary

The Canadian government rates cyber-security threats as one of seven highest. It characterises these as states (military and espionage), cybercriminals and terrorist groups. There is a coordinating team within Public Safety Canada that takes lead responsibility for formulating a response.

3.1.2 Introduction

Canada's National Cyber Security Strategy[18] was published in 2010. This was Canada's first attempt at a cross-governmental strategy. Canada's cyber-security posture is similar to its allies in the 'Five Eyes'[19] community, in that intelligence agencies are at the forefront of developing the approach.

Canada's cyber-security strategy outlines that espionage[20] (particularly from China and other Pacific Rim states) and cybercrime are the most pressing priorities within the cyber domain. This may reflect that Nortel,[21] at one time Canada's largest communications corporation, has been identified by many cyber experts as the victim of a significant level of industrial espionage.

[18] Public Safety Canada (2010).

[19] The Anglophone intelligence community of Australia, Canada, New Zealand, the UK and the USA.

[20] Freeze (2012).

[21] Marlow (2012).

3.1.3 The prioritisation of cyber threats in national risk assessment

Cyber-security is one of seven highest national security priorities approved annually by the Cabinet's Ad Hoc Committee on Security and Intelligence. It ranks alongside:

- international terrorism and extremism;
- the mission in Afghanistan;
- the proliferation of weapons of mass destruction;
- foreign espionage and interference;
- Canada's Northern Strategy; and
- international security and prosperity interests.[22]

The cyber-security strategy is built on three pillars: securing government systems; partnering to secure vital cyber-systems outside the federal government; and helping Canadians to be secure online.

3.1.4 How is the threat characterised?

The National Cyber Security Strategy characterises threat actors relevant to cyber-security in the following typology:

- military and intelligence organisations undertaking state-sponsored cyber military and espionage activities – political, economic, commercial and military purposes
- cybercriminals – identity theft, money laundering, extortion
- terrorist groups – recruitment, fundraising, propaganda, attacks

3.1.5 Entities involved in response

Canada's cyber response is led by a coordinating strategic team within Public Safety Canada, the interior ministry. They are responsible for the delivery of the strategy and ensuring an integrated approach across governmental and private actors. The principal interlocutors for executing the strategy and their roles are as follows:

- Canadian Cyber Incident Response Centre within the government Department of Public Safety – monitors threats, public safety and awareness
- Communications Security Establishment Canada (independent agency under the Ministry of Defense) – detects and discovers threats, provides intelligence and cyber-security, responds to threats against government systems
- Canadian Security Intelligence Service (CSIS) – investigates and analyses domestic and international threats to the security of Canada
- Royal Canadian Mounted Police (Integrated Cyber Crime Fusion Centre) – investigates suspected domestic and international criminal acts in cyberspace
- Canadian networks and critical information infrastructure
- Treasury Board Secretariat – responsible for the information security of the government

[22] National Defence and the Canadian Forces (2012).

- Department of National Defence and the Canadian Forces (military) – responsible for defending their own networks.

Cybercrime responsibility falls within the remit of the Royal Canadian Mounted Police, which has established an Integrated Cyber Crime Fusion Centre and Cybercrime Council to lead on policy development in this area.[23] The Royal Canadian Mounted Police also works closely with CSIS and Canada's Signals Intelligence Agency on their investigative response.

3.1.6 Policy sources

- Public Safety Canada, Government of Canada (2010) *Canada cyber-security strategy: for a stronger and more prosperous Canada*. As of 5 December 2012: http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf

3.2 Denmark

3.2.1 Summary

The Danish government estimates the cyber threat as being 'highly likely' (75–100 percent) that it will become an ever-increasing security risk. Threat is characterised according to a mixed identification of threats (terrorists) and risks (disruption or control of information technology [IT] infrastructure) and financial damage. Denmark has a model of sectoral responsibility, but leadership appears to be exercised through the Danish Security and Intelligence Service and the National High Tech Crime Centre.

3.2.2 Introduction

Denmark does not have a national cyber-security strategy in the public domain, neither is it clear that it is in the process of considering such a strategy. The Danish Defence Intelligence Service's Intelligence Risk Assessment 2011[24] dedicates a section to cyber threats and states that it is 'highly likely' (75–100 percent) that cyber threats will become an ever-increasing security risk. The Danish Defence Intelligence Service appears to have significant operational responsibility for the national security cyber threat. Danish military doctrine references cyberspace as a military battle space, but does not provide details of concrete technical and operational capacity. However, the Danish Defence Agreement 2010–2014 has called for the establishment of a cyber network operations unit.[25]

3.2.3 The prioritisation of cyber threats in national risk assessment

In addition to cyber threats being considered as 'highly likely' (75–100 percent chance), the Intelligence Service Risk Assessment places cyber threats at a level similar to that posed by Sunni extremism.

The prioritisation of risks in the National Risk Assessment – a ranking of the relative likelihood of events in the Danish Emergency Management Agency's risk assessment model (see 3.2.4) – are not published.

---

[23] Black (2011).

[24] Danish Defence Intelligence Service (2011).

[25] The Liberal Party et al. (2009, p.11).

3.2.4 How is the threat characterised?

The Intelligence Service Risk Assessment describes threats according to the motive underlying the attack. It cites financial damage, espionage, disruption or control of the IT infrastructure and electronic warfare as cyber threats, and emphasises the potential role of state-level actors in cyber-warfare.

A second source identified is the threat assessment of the Danish Security and Intelligence Service's Centre for Terror Analysis,[26] which also considers the cyber-security implications of identified terrorist threats (extremism, weapons of mass destruction, espionage, serious organised crime, Islamist terrorism).

The Danish Emergency Management Agency's risk assessment model[27] considers the impact of cyber-terrorism and IT attacks under two categories: international terrorism and "Terrorist actions against authorities, critical infrastructure assets, employees, the wider population, etc." IT attacks are included also under the 'crime' theme.

3.2.5 Entities involved in response

The Danish Security and Intelligence Service (under the Ministry of Justice) is responsible for the analysis, detection and prevention of cybercrime, in collaboration with the National High Tech Crime Centre of the Danish National Commissioner of Police, and the Ministry of Defence's Defence Intelligence Service. The Defence Intelligence Service is responsible for finding and preventing cyber threats, and is planning to build a cyber-warfare unit.[28] Public–private partnership with the owners and operators of critical infrastructure is considered a priority.

The fundamental principle of emergency preparedness and response in Denmark is that the authority, company or institution with day-to-day responsibility for a given area is also responsible for that area in the event of a major accident or disaster. This is the so-called 'sector responsibility' principle. The Danish Preparedness Act 2004 established the duty of individual ministries to ensure that there are plans for the maintenance and re-establishment of society's vital functions in their area of responsibility, in the event of accidents or disasters. This applies particularly to critical infrastructure such as electricity, IT, water and transport. While the Preparedness Act does not directly address risk analysis matters, it has an impact on how it is organised and conducted.

The National High Tech Crime Centre cooperates with the national investigation units and the Prosecution Service on the investigation and enforcement aspects of cybercrime. Conversely, the Danish Security and Intelligence Service, which is formally part of the police but reports directly to the Ministry of Justice, is responsible for gathering national and international intelligence and identifying, preventing and countering threats, including cyber threats.

---

[26] Danish Security and Intelligence Service, Centre for Terror Analysis (2012).

[27] Danish Emergency Management Agency (2006).

[28] The Liberal Party et al. (2009, p.11).

3.2.6 Policy sources

- Danish Defence Intelligence Service (2011) *Danish Defence Intelligence Service intelligence risk assessment*. As of 5 December 2012: http://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/risikovurdering2011_EnglishVersion.pdf
- Danish Government (2004) *Danish Preparedness Act*. As of 5 December 2012: http://biblio.crn.ethz.ch/risk/index.php/publications/show/236
- Danish Security and Intelligence Service, Centre for Terror Analysis (2012) *National threat assessment*. As of 5 December 2012: https://www.pet.dk/~/media/Engelsk/VTD%20NTV%20UK/NTVUK20120131pdf.ashx
- The Liberal Party, the Social Democratic Party, the Danish People's Party, the Socialist People's Party, the Conservative Party, the Radical Liberal Party, the Liberal Alliance Party (2009) *Danish defence agreement 2010–2014*. As of 5 December 2012: http://merln.ndu.edu/whitepapers/Denmark2010-2014English.pdf

3.3 Estonia

3.3.1 Summary

Estonia rates the cyber-security threat as high (4 on a 5x5 matrix of impact and likelihood). It focuses upon the effects of threats (critical infrastructure attacks or cybercrime). The Estonian Authority for Information Systems (RIA) is the lead designated authority.

3.3.2 Introduction

The 2007 distributed denial of service attacks have pushed Estonia into the spotlight with respect to cyber-security. Estonia was the first EU Member State to publish a cross-government, national cyber-security strategy in 2008 following the DDoS attacks. Estonia's threat assessment follows very much from a desire to increase resilience and manage the consequences of such attacks in future.

3.3.3 The prioritisation of cyber threats in national risk assessment

The 2011 update of the national emergency risk assessment, an integrated part of the National Security Concept, rates the likelihood of cyber-attack as "high" (4 on a 5x5 matrix of impact and likelihood). The following threats were classified in the same category: pollution, coastal pollution, epidemics. Heat waves, wildfires and mass poisoning were allocated the same degree of likelihood but less dangerous impact. The effects of a cross-border nuclear incident, industrial fires, formation or dissolution of ice and groundwater contamination were allocated the same level of impact, but with less likelihood.

3.3.4 How is the threat characterised?

The Estonia Cyber Security Strategy 2008–2013 is unique in rejecting cyber-warfare, cybercrime or cyberterrorism divisions, and instead focuses on the chosen effects of threat actors. It characterises attacks as either cyber-attacks against critical information

infrastructure or cybercrime. The strategy emphasises the necessity of a secure cyberspace in general and focuses on information systems. The recommended measures are focused on the private and/or civil sector, and on regulation, education and cooperation.

3.3.5 Entities involved in response

Since the 2007 cyber-attacks, a central authority for cyber-security has been established: RIA has coordinating powers over government efforts in cyber and related departments such as the Department of Critical Information Infrastructure Protection. RIA handles incident response, the protection of critical information infrastructures and serves as a platform for cooperation and the integration of efforts. The military has a crucial role in cyber-defence, particularly regarding close cooperation with NATO through the Estonia-hosted Cooperative Cyber Defence Centre of Excellence established in Tallinn.

On a broader European policy level, Estonian officials appear to play a key role in shaping the cyber-security debate across a number of fields (defence, legal, foreign affairs, etc.). Notably, Heli Tiirmaa-Klaar (Cyber Security Policy Advisor in the Conflict Prevention and Security Policy Directorate of the European External Action Service) recently moved from NATO headquarters to the European External Action Service, highlighting Estonia's leading role in cyber policy discussions and potentially opening the way for closer cooperation between the EU and NATO.

The IT Crimes Office of the Criminal Police sits within the Ministry of Interior. Also within the Ministry are units dedicated to crisis management, cybercrime and critical infrastructure protection, which are responsible further for coordinating Estonia's information security.

3.3.6 Policy sources

- Cyber Security Strategy Committee, Ministry of Defence (2008) *Estonia cyber-security strategy*. Accessed 4 December 2012: http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf
- Estonian Government (2010) *National security concept of Estonia*. As of 5 December 2012: http://www.mod.gov.ee/files/kmin/nodes/9470_National_Security_Concept_of_Estonia.pdf

3.4 Finland

3.4.1 Summary

Finland is at the early stages of its development, and we were not able to locate a publicly available prioritisation or assessment of the cyber-security threat. As yet there does not appear to be a single agency that leads response.

3.4.2 Introduction

Finland currently lacks special cyber-security units and a national strategy, although the development of such a strategy is in its early stages. The government stresses the importance of cooperation between public and private actors, as the latter own most of the

infrastructure, and of government collaboration in terms of response (particularly between defence and other ministries).

3.4.3 The prioritisation of cyber threats in national risk assessment

The Finnish national security strategy lists and develops the possible consequences of 13 threat scenarios, one of which is "serious disruptions to telecommunications and information systems". However, we cannot determine from these scenarios whether there is an assessment according to the relative plausibility of such an attack, or of its impact against other risks.

3.4.4 How is the threat characterised?

The strategy of the Finnish armed forces to 2025 repeatedly mentions cyber-warfare and "information warfare, network jamming and attacks" among the emerging models of conflict, along with terrorism.

The threat assessment undertaken by the Ministry of Transport and Communications lists three cyber-threat scenarios out of a total of nine scenarios of severe disruption of critical IT infrastructure, but does not publish the detailed risk assessment behind these scenarios.

Cyber threats are defined by the national security strategy as "a threat against interdependent networks", without describing a typology of actors. The Ministry of Transport's assessment classifies threats according to type of impact, and includes three categories of attacks classified as a "special situation directly concerning ICT [information and communication technology] infrastructure": political, economic and military pressure resulting in the disruption of internet-based services; terrorist attacks; and the use of military force.

3.4.5 Entities involved in response

In the absence of a specialised agency, responsibility for cyber-security policy and implementation is distributed among government departments. The Ministry of Finance is responsible for driving and developing the information security of the Government of Finland, with the Ministry of Defence in charge of its own systems, the Ministry of Transport and Communications in charge of critical infrastructure, and the Ministry of Interior in charge of internal security. Although to date the Finnish government does not have a national steering group in charge of cyber-security matters, the military's Cyber Defence Unit is connected to military and internal intelligence, and has responsibility for both defensive and offensive aspects.

Law enforcement responsibilities in this area are undertaken by the Cybercrime Investigations Unit within the National Bureau of Investigations. This unit has the authority to investigate offences committed against computer systems and data, as well as offences committed through computer systems. The cyber unit cooperates with the CERT, Cybercrime Intelligence Unit and Crime Laboratory, and takes charge of coordinating the efforts of investigations that involve multiple law enforcement authorities, such as customs officers and border guards. It provides its resources and plays a strategic role in investigations in one locality. In these cases, the leading role is given to local police units.

3.4.6 Policy sources

- Ministry of Defence of Finland (2010) *Security strategy for society*. As of 5 December 2012: http://www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf

- Ministry of Defence (2006) *Securely into the future: Ministry of Defence strategy 2025*. As of 5 December 2012: http://www.defmin.fi/files/674/Securely_into_the_future_-_strategy_2025.pdf
- Ministry of Transport and Communications (2011) *Enhancing the usability and availability of information infrastructure essential for securing the vital functions of society: final report*. As of 5 December 2012: http://www.lvm.fi/c/document_library/get_file?folderId=1551284&name=DLFE-11788.pdf&title=Julkaisuja%203-2011

3.5 France

3.5.1 Summary

We were unable to obtain a publicly available typology for France. Cyber is an important feature of the French security landscape and response is shaped by a leading ministerial agency – the French Network and Information Security Agency (Agence Nationale de la Sécurité des Systems d'Information, ANSSI).

3.5.2 Introduction

In recent years, cyber security has been given an increasingly prominent position in French defence and security strategy: ANSSI was formed in 2009 to protect public institutions, companies and individuals. However, French annual spending on cyber-defence only amounts to €75m and lags far behind the USA's US$10 billion.[29] A 2012 French senate report considers that public and private sectors both lack sufficient cyber-defences.[30]

3.5.3 The prioritisation of cyber threats in national risk assessment

A 2008 White Paper on defence and national security categorises cyber-attacks, along with "nuclear deterrence, ballistic missiles, SSBNs [ballistic missile submarines] and SSNs [fast attack submarines]", as a major threat to the national territory.[31]

3.5.4 How is the threat characterised?

Specific incidents over the past year have demonstrated the dangers of cybercrime in France. In December 2011, the Ministry of Finance was the victim of a cyber-attack which targeted files on the G20 summit hosted in Paris in February 2012. French investigators concluded that the attack probably originated from Chinese computers and that it was unprecedented in its scale and impact. In May 2012, the cyber threat was once more brought to the attention of Francois Hollande's government when websites for French companies and the presidency were hacked.

More generally, the French cyber-security landscape features a number of vulnerabilities and threats emanating from state and non-state actors. Critical infrastructures, such as energy distribution or the health sector, are areas which have proven particularly

[29] *DiploNews* (2012).

[30] Committee on Foreign Affairs, Defence and Armed Forces of the Senate (2012).

[31] Présidence de la République (2008, p. 306).

susceptible to cyber-attacks in recent years.[32] A 2011 ENISA report deems 'botnet' networks and the resulting spam and/or related attacks (phishing or pharming) to be the main contemporary network and information security risks in France.[33] French websites face millions of daily small-scale attacks, resulting in appropriation of personal data, espionage of scientific, economic and commercial assets of companies by competitors or foreign powers, trade in counterfeit goods, service disruption and even loss of life. Such acts are allegedly perpetrated by terrorists, major national and transnational criminal networks, narcotics traffickers, competitor industries and hostile states.

China poses a particularly formidable threat: Roger Romani, rapporteur of the French Senate Cyber Defence Report, echoed US cyber-security adviser Richard Clarke's concerns that electronic equipment imported from China could be implanted with 'logic bombs', trapdoors and 'Trojan horses', all of which could be activated on command remotely, exposing France to cyber-warfare and cyber-sabotage.

3.5.5 Entities involved in response

French cyber-defence efforts are all centralised under ANSSI, an umbrella organisation with a budget of €75m and 230 personnel.[34] The agency is placed under the authority of the prime minister and attached to the Secretary General for National Defence. ANSSI also has bilateral cyber-cooperation agreements with the relevant authorities in Germany (Federal Office for Information Security, BSI) and Estonia (RIA).[35] The 2012 French Senate Report confirms effective coordination of efforts between ANSSI, the military and the Secrétariat Général de la Défense et de la Sécurité Nationale (General Secretariat for Defense and National Security). However, it also notes that France still lags behind Germany, the UK and the USA with regard to its budget, personnel numbers and scope.[36]

Besides the Secretariat and ANSSI, several departments have policy roles: the Ministry of Defence; Direction Générale de l'Armement; Direction de la Protection et de la Sécurité de la Défence; Ministry of the Interior; Direction Centrale du Renseignement Intérieur; Office Central de Lutte Contre la Criminalité Liée aux Technologies de l'Information et de la Communication (Central Office for the Fight Against Crime Linked to Information Technology and Communication); and specialised services of the National Gendarmerie, particularly the Service Technique de Recherches Judiciaires et de Documentation (Technical Service Judicial Research and Documentation) and the Institut de Recherche Criminelle de la Gendarmerie Nationale (Electronic Criminal Research Institute of the National Gendarmerie).

---

[32] Committee on Foreign Affairs, Defence and Armed Forces of the Senate (2012).

[33] ENISA (2011a).

[34] Committee on Foreign Affairs, Defence and Armed Forces of the Senate (2012).

[35] Committee on Foreign Affairs, Defence and Armed Forces of the Senate (2012).

[36] With only 230 employees, ANSSI is relatively understaffed compared to its counterparts in the UK (700 employees) and Germany (500 employees). See Committee on Foreign Affairs, Defence and Armed Forces of the Senate (2012).

3.5.6 Policy sources

- Présidence de la République (2008) *The French White Paper on defence and national security*. As of 5 December 2012: http://www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf
- Committee on Foreign Affairs, Defence and Armed Forces of the Senate (2012) *Cyberdefence: a global issue, a national priority*. As of 5 December 2012: http://www.senat.fr/rap/r11-681/r11-6811.pdf

3.6 Germany

3.6.1 Summary

There is no publicly available o prioritisation of the cyber-security threat for Germany. However, threat actors are characterised from the types of context in which they might operate, such as war, terrorism and crime, as well as natural hazards and technical failure of systems. Leadership for response appears to be split between the Federal Ministry of the Interior, and a newly-established National Cyber Defence Centre (NCAZ).

3.6.2 Introduction

Cyber is a critical component of German preventative security strategy.[37] Although German cyber strategy has lagged behind similar initiatives in the UK and the USA, the publication of a federal Cyber Security Strategy for Germany by the Federal Ministry of the Interior in early 2011 marks a step forward.[38] The strategy resulted in the creation of two new bodies: the NCAZ and the National Cyber Security Council.

3.6.3 The prioritisation of cyber threats in national risk assessment

The government considers data security "an existential question of the 21st century", and "the central common challenge for state, business and society" in Germany.[39]

3.6.4 How is the threat characterised?

As a nation that uses highly industrialised, complex technologies and which relies on sophisticated organisational structures, Germany is particularly vulnerable to critical infrastructure attacks and faces a range of threats.[40] These threats are classified by the German federal government within a tripartite framework, falling into the categories of terrorism, crime and war; natural hazards; and technical failure or human error.[41]

First, since the 9/11 attacks the international terrorist threat has been a key driver of the federal government's efforts to achieve security. Such threats, both within and outside Germany, are facilitated by sabotage, espionage and other forms of criminal activity which may have a cyber component.[42] Further intentional threats of this nature include credit

[37] Committee on Foreign Affairs, Defence and Armed Forces of the Senate (2012).

[38] Federal Ministry of the Interior (2011).

[39] ENISA (2011b).

[40] Federal Ministry of the Interior (2011).

[41] Federal Ministry of the Interior (2011).

[42] Federal Ministry of the Interior (2009).

card fraud, botnets, electronic viruses, worms and Stuxnet-type attacks against critical infrastructure.[43] Second, global climate change has intensified the impact of extreme weather events on infrastructure, even in the temperate latitude zones of Central Europe. These effects may be amplified by a cyber-security failure. Third, the operability of critical infrastructure is endangered by technical failure or human error.

All such threats may trigger so-called 'domino effects' and 'cascade effects' which can paralyse sectors of society, harming individuals, the economy and confidence in political leadership.

3.6.5 Entities involved in response

In Germany, the Federal Ministry of the Interior has ultimate responsibility over policy development and implementation. The Federal Office for Civil Protection and Disaster Assistance, Federal Office for Information Security (BSI) and Federal Criminal Police Office are all placed under its supervision. These organisations are responsible for conducting threat assessments and analyses, and formulating protective responses.

German cyber-defence efforts take place within the framework of the Federal Ministry of the Interior's 2011 Federal Cyber Security Strategy for Germany, and are therefore centralised by the newly-created NCAZ, established to pool the resources of different government agencies including the federal police and Federal Intelligence Service. NCAZ reports to the Federal Office for Information Security, and cooperates directly with the Federal Office for Civil Protection and Disaster Assistance and the Federal Office for the Protection of the Constitution. The Federal Criminal Police Office, federal police, Customs Criminological Office, Federal Intelligence Service, Bundeswehr and authorities supervising critical infrastructure operators all participate in NCAZ within the framework of their statutory tasks and powers. By law, Bundeswehr University is the only responsible authority for protection of the IT systems of the armed forces.

NCAZ acts as the coordinating platform in charge of handling cyber incidents, and submits recommendations to the National Cyber Security Council, which is also a product of the 2011 Federal Cyber Security Strategy for Germany. The Council was established to maintain cooperation within the federal government, and between the public and the private sector. It includes the federal chancellery and a state secretary from each of the Federal Foreign Office, Federal Ministry of the Interior, Federal Ministry of Defence, Federal Ministry for Economics and Technology, Federal Ministry of Justice, Federal Ministry of Finance, Federal Ministry of Education and Research and representatives of the federal *Länder*.

However, strict constitutional separation of civil and military responsibilities creates a challenge for an integrated approach. Particularly in defence and intelligence, coordination and information sharing are rapidly subject to senior-level approval requirements, meaning that only the most critical issues are likely to benefit from truly integrated action. That said, the Bundeswehr University can leverage its academic status to act as a backchannel and convene and discuss relevant agencies more easily, thus facilitating the exchange of information and views. It has been reported that the military command for strategic reconnaissance (Kommando Strategische Aufklärung [Strategic Reconnaissance

[43] ENISA (2011b).

Command], part of military counter-intelligence) has trained and set up an information and net operations section, employing 76 people at the time (as reported by *Der Spiegel*).

Germany also has a strong CERT network, cutting across geographical areas and industry sectors. All are part of the national CERT-Verbund network (federation of CERTs) aimed at coordinating all national CERTs and sharing best practice.

3.6.6 Policy sources

- Federal Ministry of the Interior (2009) *National strategy for critical infrastructure protection (CIP Strategy)*. As of 5 December 2012: http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf
- Federal Ministry of the Interior (2011) *Cybersecurity strategy for Germany*. As of 5 December 2012: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

3.7 Netherlands

3.7.1 Summary

The Netherlands classifies cyber-security as a 'high priority'. Cyber-security threats are defined according to a set of actors including states, private individuals, professional criminals, terrorists, hacktivists, script kiddies, cyber-researchers and internal actors, as well as non-actor-based threats (eg failure of systems). The National Cyber Security Centre is the lead authority for response.

3.7.2 Introduction

In early 2011, the Dutch government published its National Cyber Security Strategy, prepared with contributions from a broad range of public and private parties, research institutes and social organisations. The strategy has five components:

1. linking and reinforcing initiatives;
2. promoting individual responsibility;
3. creating public–private partnerships;
4. pursuing international cooperation; and
5. striking a balance between self-regulation and legislation.

3.7.3 The prioritisation of cyber threats in national risk assessment

The strategy classifies cyber-security as a "high priority", but its statement that cyber-defence initiatives "will be dealt with within the existing budgets" is reflective of government financial constraints.[44] The 2010 national risk assessment places state-on-state cyber conflict in the same category as right-wing extremism, medium or high-intensity flu pandemics and heatwaves or coldwaves.

[44] Dutch Government (2011, pp. 3, 9).

3.7.4 How is the threat characterised?

The National Cyber Security Centre's Cyber Security Assessment 2012 identifies and analyses a range of cyber threats, actors, tools and motives.[45] Information-related threats include the publication of confidential data, digital identity fraud, digital espionage, system-related threats (disruption of vital infrastructure or online services) and indirect threats (disruption of business operations resulting from malware infection, spam or hoax). Emergencies (arising from fire or water damage, or natural disasters) or hardware or software failure also can lead to disruption of business operations.

According to the report, 'digital espionage' by China, Iran, Russia and other hostile states and attacks implemented by professional criminals are the most pressing cyber threats. By contrast, other threat sources – internal actors, cyber-researchers, script kiddies, terrorists and hacktivists – are less dangerous. The National Cyber Security Centre classifies digital espionage, malware infection and spam as high threats for government and private organisations, while digital identity fraud poses a medium threat to citizens.

The report further notes that the most damaging technical tools wielded by threat groups continue to be exploits, malware and botnets. Cybercriminals have set their sights increasingly on the Apple Macintosh platform, recently developing a botnet of more than 500,000 Apple computers. In addition, dangerous new developments have been noted in ransom-ware, exploit kits and the misuse of web mail accounts to send spam and malware.

Threat actors are driven by a range of motivations. While states often target government bodies to improve their geopolitical position, private organisations attack their own competitors to advance their information position. Professional criminals are driven by the promise of monetary gain; terrorists strive to secure ideological and political objectives; script kiddies are motivated by opportunism and the desire to experiment; cyber-researchers seek to profile themselves and expose weakness; and internal actors act out of a sense of revenge, carelessness or incompetence. Of these threat groups, states, private organisations and internal actors have the highest volume of resources, and attacks launched by terrorists, hacktivists and cyber-researchers are the most visible.

In the Netherlands' case it is possible to identify how appreciation of the risks evolved from the national level risk assessment conducted in 2010 to the one conducted in 2012. Below we briefly summarise how cyber threats were identified in these assessments.

2010 national risk assessment. In the 2010 national risk assessment, a cyber-attack scenario is included where a state is involved in a "large-scale and coordinated" attack. Two scenarios are identified: the interruption of Dutch internet exchanges and cyber-conflict; and disruption of internet protocol networks.

Cyber-attack scenario: probability = "likely" (D; 4 on a scale from 1 = improbable to 5 = very probable; impact ranging from zero to severe).

This assessment places cyber-conflict in the same category of probability as right-wing extremism, medium or high-intensity flu pandemics and heatwaves or coldwaves.

[45] National Cyber Security Centre, Ministry of Security and Justice (2012).

The most severe impact of the scenario is at the psychosocial level, where it is classified as D = "very serious consequences" (4 out of 5 on a scale ranging from limited effects (= 1) to catastrophic consequences (= 5). Along with "disruption of IP internet protocol] networks", this risk is among the highest projected impacts in this aspect, along with "unrest in problem areas" and "oil geopolitics".

Suspension of internet connections: Probability = A (very unlikely) with a low impact, limited to costs.

Disruption of internet protocol networks: Probability = C (probable) at the same level of risk as animal rights activism or criminal infiltration in the public sector. The social-psychological and cost-related consequences are categorised as D = very serious.

2012 cyber-security risk assessment. Table 3 indicates the threat actor model constructed for this assessment.

Table 3: Threat actor model and activity against sectors for the 2012 cyber-security risk assessment

Threat Actors	Government	Private	Citizen
States	Digital espionage	Digital espionage	Digital espionage
Private organisations		Digital espionage	
(Professional) criminals	Disruption as a result of malware infection and spam	Disruption as a result of malware infection and spam	Disruption as a result of malware infection and spam
		Digital (identity) fraud	Digital (identity) fraud
	Blackmail	Blackmail	Blackmail
	Disruption of online services	Disruption of online services	Disruption of online services
Terrorists	Sabotage	Sabotage	Sabotage
Hacktivists	Publication of confidential data		
		Publication of confidential data	Publication of confidential data
	Disruption of vital infrastructure	Disruption of vital infrastructure	
	Disruption of online services	Disruption of online services	
	Hoax	Hoax	Hoax
	Disruption of online services	Disruption of online services	
Script kiddies	Publication of confidential data	Publication of confidential data	
Cyber-researchers		Blackmail	
Internal actors	Fire, water damage and natural disasters	Fire, water damage and natural disasters	
Non-actor	Failure and/or absence of hardware	Failure and/or absence of	

	and software	hardware and software

3.7.5 Entities involved in response

The main actors are the National Cyber Security Centre (under the Ministry of Justice) and High Tech Crime Team of the national police, and the Cyber Taskforce of the Ministry of Defence, alongside general and military intelligence organisations (the Algamene Inlichtingen- en Veiligheidsdienst [AIVD] and Militaire Inlichtingen- en Veiligheidsdienst [MIVD]).

The National Cyber Security Strategy resulted in the establishment of the National Cyber Security Centre in January 2012 and the foundation of the Cyber Security Council in mid-2011. The Council sets priorities for the tackling of information and communication technology (ICT) threats, considers the need for further research and development, and then establishes the best way to share this knowledge with the collaborating public and private parties.

The Cyber Taskforce has been operational within the Ministry of Defence since 1 January 2012. It operates on the basis of four lines of operation: defensive and offensive operations, information; education and training; and research and development (R&D). Based on development of the Vision on Cyber Operations (*Uitwerking visie op cyberoperations*) in June 2012, efforts are being made to achieve the foundation of a Defence Cyber Expertise Centre (Defensie Cyber Expertise Centrum) at the end of 2013, and the creation of a Defence Cyber Command (Defensie Cyber Commando) at the end of 2014.

The AIVD provides targeted support to specific organisations within the government and private sector when monitoring information systems. In addition, the National Police Services Agency, National Public Prosecutor's Office (Landelijk Parket), banks and Dutch Centre for Protection of the National Infrastructure are working together in the Electronic Crimes Taskforce – also referred to as the 'Banks Team'.[46]

3.7.6 Policy sources

- Dutch Government (2011) *The national cyber-security strategy (NCSS): success through cooperation*. As of 5 December 2012: http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011
- Ministry of Security and Justice (2010) *National risk assessment 2010*. As of 5 December 2012: http://www.infosecisland.com/blogview/13379-Cyber-Conflict-in-Dutch-National-Risk-Assessment-of-2010.html
- National Cyber Security Centre, Ministry of Security and Justice (2012) *Cyber security assessment Netherlands: CSBN-2*. As of 5 December 2012: https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/trend-reports/the-english-version-of-the-cyber-security-report-2012.html

[46] National Cyber Security Centre, Ministry of Security and Justice (2012).

3.8 Russian Federation

3.8.1 Summary

We were unable to locate details of the prioritisation of cyber threats in the Russian Federation. Threats are broadly characterised as internal (crime and corruption) and external (state, terrorists, foreign competition). The lead authority for response appears to be between the Security Council of the Federation, Ministry of Defence and other organisations (eg the national system for information protection and the intelligence community).

3.8.2 Introduction

According to the Information Security Doctrine of the Russian Federation, "Based on the national interests of the Russian Federation in the information sphere, the state forms its strategic and current domestic and foreign policy objectives for ensuring information security".[47] In recent years the Russian Federation has adopted a number of high-level policy documents relating to cyber-security in the national and international setting. However, the methodology and results of the risk assessment conducted to support the policy are not publicly available.

3.8.3 The prioritisation of cyber threats in national risk assessment

In the section of the Russian Federation's National Security Strategy to 2020[48] concerning emerging major threats (to the social and economic progress of the country and to national sovereignty), cybercrime and cyber-conflict are listed alongside violent extremism, one-sided use of force in international relations, demographic change, environmental risks and transnational organised crime.[49] Enhancing the technological capabilities of the armed forces is among the mid-term priorities, in the context of finding alternatives to a defence based on nuclear deterrence. This priority has been further defined by a programmatic initiative on the reform of the armed forces.[50]

Similarly the strategy, which aims to implement the National Security Strategy for critical infrastructure protection, lists cyber-attacks among the ten most prominent threats to critical infrastructure protection, but does not disclose assessment of the threat.[51]

On the international level, the Russian Federation has presented a controversial Draft Convention on International Information Security to the United Nations, detailing its views on the nexus between state sovereignty and international cyber-security, and stressing the importance of the maintaining sovereignty over initiatives to fight cybercrime.[52]

---

[47] Government of the Russian Federation (2000, point 1).

[48] Government of the Russian Federation (2009, point 10).

[49] Government of the Russian Federation (2009, point 10).

[50] Government of the Russian Federation, Ministry of Defence (2011).

[51] Security Council of the Russian Federation (2012).

[52] Draft Convention on International Information Security, Article 5.

3.8.4 How is the threat characterised?

The Information Security Doctrine of the Russian Federation characterises threats according to their place of origin, between internal and external.[53] Internal threats refer to the challenges posed by the generic lack of adequate funding and governance structures, as well as crime and corruption within the country. External threats refer to the actions of states (conducting espionage with political, economic, industrial or military motivations) and terrorist organisations, but also foreign competition on the IT markets including R&D, selling and access to the latest technology. A theme of particular salience in Russian cyber-security policy, similar to the Draft Convention, is the view of alliances of foreign states as a threat. The Russian Federation sees other states' development of information war concepts enabling attacks on other sovereign states[54] as a key threat issue.

3.8.5 Entities involved in response

Cyber-security policy is defined by the Security Council of the Federation, chaired by the president. Implementation of guidelines is shared between the Ministry of Defence, which also controls the systems for certifying information protection tools (Federal Service for Technical and Export Control), the national system of information protection (the responsibility of the Ministry for Civil Defence) and the intelligence community, including the Centre for Licensing, Certification and Protection of State Secrets of the Federal Security Service and the External Intelligence Service. There is no information available relating to law enforcement authorities' possession of specialised cyber-capabilities.

3.8.6 Policy sources

- Government of the Russian Federation (2000) *Information security doctrine of the Russian Federation*. As of 5 December 2012: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument
- Government of the Russian Federation (2009) *Russia's national security strategy to 2020*. As of 5 December 2012: http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020
- Government of the Russian Federation, Ministry of Defence (2011) *Convention on international information security*. As of 5 December 2012: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument

[53] Government of the Russian Federation (2000, point 3).

[54] Article 4 of the Draft Convention on International Information Security.

3.9 United Kingdom

3.9.1 Summary

The UK places cyber-security as a Tier 1 national security priority (one out of four).[55] The threat is characterised as a number of sources including states, terrorists and criminal organisations. The Office for Cyber Security and Information Assurance, a cabinet-level organisation, has lead responsibility for orchestrating a response.

3.9.2 Background

The UK published a first strategy, *Cyber Security Strategy of The United Kingdom: Safety, Security and Resilience in Cyberspace* in June 2009,[56] and followed up with a second document, *The United Kingdom Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*[57] less than two and a half years later. The second (and current) cyber-security strategy is shaped by the tenets of the Strategic Defence and Security Review 2010. This document re-evaluated the importance of cyber-security in a fundamental way.

3.9.3 The prioritisation of cyber threats in national risk assessment

The current (2011) National Cyber Security Strategy identifies improving cyber-security as a Tier 1 risk (one of four Tier 1 risks). A Tier 1 risk is "judged to be the highest priority for UK national security over the next five years, taking into account both likelihood and impact". A further eleven Tier 2 and Tier 3 risks are articulated, however the Strategic Defence and Security Review suggests that "overall, the risks in the top priority band drive a prioritisation of capabilities". The articulation of cyber as a Tier 1 risk paved the way for cyber-security related agencies to be allocated a four-year budget of £650m.

3.9.4 How is the threat characterised?

The UK National Risk Register,[58] the non-classified version of the National Risk Assessment performed yearly by the Cabinet Office, lists two types of cyber-attack as pertinent within the Tier 1 characterisation of cyber threat: cyber-attacks targeting infrastructure; and cyber-attacks resulting in breach of data confidentiality.

Cyber-attacks on infrastructure have a score of 3 out of 5 of relative impact, and a medium–low relative plausibility of occurring over the next five years (the same relative impact level, but lower plausibility as small-scale Chemical, Biological. Radiological and Nuclear (CBRN) attacks, attacks on infrastructure, attacks in crowded places and attacks on transport systems; the same relative plausibility but a lower relative impact than

---

[55] Tier-1 threats comprise: international terrorism affecting the UK or its interests, including a CBRN attack by terrorists and/or a significant increase in the levels of terrorism relating to Northern Ireland; hostile attacks upon UK cyberspace by other states and large-scale cybercrime; an international military crisis between states, drawing in the UK, its allies as well as other states and non-state actors; a major accident or natural hazard that requires a national response, such as severe coastal flooding affecting three or more regions of the UK, or an influenza pandemic (see Cabinet Office, 2010).

[56] Cabinet Office (2009).

[57] Cabinet Office (2011).

[58] Cabinet Office (2012).

catastrophic terror attacks), or comparable to the relative likelihood of major transport accidents.

Cyber-attacks resulting in breach of data confidentiality have a score of 1 out of 5 of relative impact, and a high relative plausibility of occurring over the next five years. This means that they are the lowest in terms of relative impact among the threats considered, but have the highest relative plausibility – the same as attacks on transport systems. It is the lowest impact and one of the two most plausible risks among those assessed.

The UK National Risk Register[59] provides a number of sources of threat:

- states – economic, industrial and military espionage and disruption;
- terrorist groups – propaganda, fundraising and planning; and
- politically active groups – disruption, profile-raising for hacktivists, reputational damage to target.

The November 2011 cyber-security strategy[60] further provides a characterisation of threat actors as criminals, nation-states engaged in intelligence and military operations, economic, military or industrial espionage or disruption, and 'patriotic' hackers acting on states' behalf to spread misinformation. In addition, terrorist groups involved in propaganda and fundraising activities and hacktivists (politically motivated groups) acting to cause reputational damage are highlighted.

3.9.5 Entities involved in response

The UK has a dedicated Office of Cyber Security and Information Assurance (OSCIA), which supports the Minister for the Cabinet Office and the National Security Council. This body coordinates a larger cross-government effort, and OCSIA's role is to harness close cooperation and coordination between the various national-level agencies and departments and promote a common policy approach. OCSIA, along with the Cyber Security Operations Centre, works with lead government departments and agencies such as the Home Office, Ministry of Defence, Government Communications Headquarters (GCHQ, the government communications intelligence agency), Communications Electronics Security Group, Centre for the Protection of National Infrastructure and Department for Business, Innovation and Skills in implementing the government's cyber-security programme. In addition, security policies involve the communications regulator, Ofcom, the Information Commissioner's Office and police departments such as the Serious Organised Crime Agency and the Police Central e-crime Unit. The Centre for the Protection of National Infrastructure facilitates the public–private partnership efforts in the UK.

The distribution[61] of the £650m cyber-security programme budget suggests that the British intelligence community is a key player in cyber-security issues, with a particularly relevant role for GCHQ, which hosts the Cabinet's Cyber Security Operations Centre.

---

[59] Cabinet Office (2012).

[60] Cabinet Office (2011).

[61] Intelligence and Security Committee (2011).

The November 2011 cyber-strategy gives detail on the respective roles of law enforcement: it announced the creation of a cybercrime unit for the upcoming National Crime Agency (previously handled by the Serious Organised Crime Agency [SOCA]) to be set up by 2013. In the interim, the Serious Organised Crime Agency and the e-Crime Unit of the Metropolitan Police remain the dedicated agencies for cybercrime.

3.9.6 Policy sources

- HM Government (2010)*Securing Britain in an age of uncertainty: the strategic defence and security review*. As of 5 December 2012: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf
- Cabinet Office (2009) *Cyber security strategy of the United Kingdom: safety, security and resilience in cyber space*. As of 5 December 2012: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf
- Cabinet Office (2010) *A strong Britain in an age of uncertainty: the national security strategy*. As of 5 December 2012: https://update.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf
- Cabinet Office (2011) *The UK cyber-security strategy: protecting and promoting the UK in a digital world*. As of 5 December 2012: http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf
- Cabinet Office (2012) *National risk register of civil emergencies*. As of 5 December 2012: http://www.cabinetoffice.gov.uk/sites/default/files/resources/CO_NationalRiskRegister_2012_acc.pdf
- Intelligence and Security Committee (2011) *Annual Report 2010–2011*. As of 5 December 2012: http://www.official-documents.gov.uk/document/cm81/8114/8114.pdf

3.10 United States of America

3.10.1 Summary

The USA places cyber-security as one of four national security priorities. The director of the Federal Bureau of Investigation (FBI) recently noted that cyber threats have the potential to equal or surpass the threat from terrorism in the near future. Four types of actors are characterised: criminal hackers, organised criminal groups, terrorist networks and advanced nation-states. Responsibilities for leading policy are broadly distributed, but there is an Information and Communications Infrastructure Interagency Policy Committee that takes a coordinating role.

3.10.2 Introduction

The engagement of the administration in harnessing executive powers in this domain was marked with the release of the 2003 White House National Strategy to Secure Cyberspace. This initiative was integral to a wider Department for Homeland Security National Security Review undertaken after 9/11. Cyber-security policy has continued to evolve in

the USA, its emphasis shifting from non-state terrorism to state actors' activities with the 2010 US National Security Strategy. [62]

3.10.3 The prioritisation of cyber threats in national risk assessment

The importance of the threats posed in the cyber domain has been a persistent theme at the top of US government across federal agencies for at least a decade. However, the way in which the threat has been characterised has changed in that period. The emphasis has shifted from non-state terrorism to state actors' activities, and from a predominantly political to an economic concern.

In February 2012, the Director of National Intelligence, James Clapper, noted to a House Select Intelligence Committee on worldwide threats: "We all recognize [cyber-attacks] as a profound threat to this country, to its future, to its economy, to its very being."[63] In the same session, FBI Director Robert S. Mueller noted that the cyber threat is growing and is crucial to address: "I do believe cyber threats will equal or surpass the threat from terrorism in the near future."[64]

The nature of US policymaking has meant that processes of development of cyber strategies and action plans have been fragmented. However, there now exists a broad web of national plans that establish cyber standards and targets.[65]

The focus of the cyber threat debate continues to develop, and over the last 18 months it has shifted to encouraging private actors to increase their efforts to protect their information infrastructures. Agencies and the administration continue to lobby Congress for regulation and the enactment of a comprehensive framework on cyber-security: a recent attempt to pass a Cybersecurity Act, placing onus on private enterprise to ensure the protection of their networks, failed. President Barack Obama's administration has stated an intention to fortify the security of critical cyber systems through his executive powers, although lobbying from interests that see the regulation of private networks as economically damaging are likely to continue.

3.10.4 How is the threat characterised?

The characterisation of threat provided by US strategy documents varies over time and according to the agency articulating the threat. The comprehensive 2009 Cyberspace Policy Review outlines cyber-security strategy to secure digital infrastructure from attack. In May 2011, the USA also released its International Strategy for Cyberspace[66] to clarify and unify its approach to international partners on cyber-security.

The comparison of cyber threats with other threats is best illustrated by in the Department of Homeland Security's 'all hazards' approach to strategic threat assessment, as outlined in

---

[62] The White House (2010).

[63] Daniel (2012).

[64] Daniel (2012).

[65] *The Economist* Intelligence Unit and Booz Allen Hamilton (2012).

[66] The White House (2011a).

the December 2011 Strategic National Risk Assessment in Support of PPD 8[67] (unclassified summary). This document considers cyber-attacks to be in the top echelon of threats facing the USA, and for which the country must prepare. The Strategic National Risk Assessment not only considers cyber threats in isolation, but also notes the impact that they have in shaping other threats: "Cyber attacks can have their own catastrophic consequences and can also initiate other hazards, such as power grid failures or financial system failures, which amplify the potential impact of cyber incidents."[68] Cyber threats articulated at the top level of threat include:

- cyber-attack against data – which seriously compromises the integrity or availability of data (the information contained in a computer system or data processes resulting in economic losses of a $1 billion or greater);
- cyber-attack against physical infrastructure – an incident in which a cyber-attack is used as a vector to achieve effects which are beyond the computer (ie kinetic or other effects) resulting in one fatality or greater, or economic losses of $100m or greater).

There is a degree of persistence in US legislators' and policymakers' characterisation of actors posing a threat to US interests, although the emphasis has changed. The Senate Armed Services Committee's intelligence community annual threat assessment in February 2008[69] outlines that the threat emanates from states (including China and Russia) for the targeting and disruption of IT infrastructure, and nation-states and criminals engaged in industrial espionage and terrorist organisations (including Al-Qaida, Hamas and Hezbollah). The 2011 US International Strategy for Cyberspace[70] evolves the discussion of actors characterising cybercriminals or states *and their proxies* as major threats.

3.10.5 Entities involved in response

Responsibilities for leading policy are broadly distributed in the US model. Policy leads are best discussed as applying to a number of policy domains.

Military and capabilities. Within the Department of Defense, the United States Northern Command (USNORTHCOM) coordinates and provides forces for Defence Security Cooperation Agency operations. The United States Strategic Command (USSTRATCOM), through the United States Cyber Command (USCYBERCOM), is responsible for synchronising, planning and executing cyber operations. USCYBERCOM directs the operations and defence of specified Department of Defense networks and when directed, conducts full-spectrum military cyberspace operations in order to enable actions in all domains for military networks.[71]

---

[67] Department of Homeland Security (2011).

[68] Department of Homeland Security (2011).

[69] McConnell (2008).

[70] The White House (2011a).

[71] The White House (2011b, pp. 12–14, 28–30). In his master's thesis, 'Expanding the Department of Defense's Role in Cyber Civil Support', Kevin Donovan (2011) is critical of the separation of international and homeland domains in critical infrastructure protection.

Critical national infrastructure. The Department of Homeland Security is the primary agency responsible for defensive actions for the rest of government networks. It coordinates efforts to protect and defend critical infrastructure, and coordinates the nation's overall critical infrastructure protection efforts, including cyber infrastructure, by working in cooperation with designated, sector-specific agencies within the Executive Branch through the National Cyber Security Center.[72]

In addition, the USA has established a number of public–private partnerships on cyber-security, including the National Cyber Security Partnership. Both the Department of Defense and Department of Homeland Security have in place public–private partnership arrangements.

Investigative and intelligence. In 2008, the Bush administration mandated the National Cyber Investigative Joint Task Force[73] to be the focal point for all government agencies to coordinate, integrate and share information related to all domestic cyber threat investigations. The FBI is responsible for developing and supporting the task force, which includes more than 20 intelligence agencies and law enforcement agencies.

Overall strategic direction. The administration's 2012 Cyberspace Policy Review tabled a set of actions for reviewing the cyberdefence system established by George W. Bush's 2008 Comprehensive National Cyber Security Initiative (more interagency coordination, counter-intelligence and awareness-raising, among others), but the Senate has failed to reach an agreement over its implementation to date.[74] The administration already has established an Information and Communications Infrastructure Interagency Policy Committee, chaired by the National Security Council and Homeland Security Council, as the primary policy coordination body for issues related to achieving an assured, reliable, secure and survivable global information and communications infrastructure and related capabilities.

The Cyberspace Policy Review also called for the appointment of a cyber-security policy official at the White House, reporting to the National Security Council to coordinate the nation's cyber-security-related policies and activities. This individual would chair the Information and Communications Infrastructure Interagency Policy Committee, and lead a strong process in consultation with other elements of the Executive Office of the President to resolve competing priorities and coordinate interagency development of policies and strategies for cyber-security. The review called for this official to participate in all appropriate economic, counterterrorism and science and technology policy discussions to inform them of cyber-security perspectives.

3.10.6 Policy sources

- Bush, G. W. (2003) *Homeland security presidential directive 7: critical infrastructure identification, prioritization and protection*. As of 5 December 2012: http://www.dhs.gov/homeland-security-presidential-directive-7#top

[72] The system was created by the National Strategy to Secure Cyberspace; it was augmented further later that year in Homeland Security Presidential Directive 7 (Bush, 2003).

[73] Federal Bureau of Investigation (2012).

[74] The White House (2009).

- Bush, G. W. (2008) *The comprehensive national cybersecurity initiative (CNCI)*, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23): Cyber Security and Monitoring
- Department of Homeland Security (2011) *The strategic national risk assessment in support of PPD 8: a comprehensive risk-based approach toward a secure and resilient nation*. As of 5 December 2012: http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf
- Federal Bureau of Investigation (2012) *National Cyber Investigative Joint Task Force*. As of 5 December 2012: http://www.fbi.gov/about-us/investigate/cyber/ncijtf
- McConnell, M. J. (2008) *Annual threat assessment of the intelligence community for the Senate Armed Services Committee*. As of 5 December 2012: http://www.armed-services.senate.gov/statemnt/2008/February/McConnell%2002-27-08.pdf
- The White House (2003) *The national strategy to secure cyberspace*. As of 5 December 2012: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf
- The White House (2009) *Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure*. As of 5 December 2012: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
- The White House (2010) *National security strategy*. As of 5 December 2012: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
- The White House (2011a) *International strategy for cyberspace: prosperity, security and openness in a networked world*. As of 5 December 2012: http://info.publicintelligence.net/WH-InternationalCyberspace.pdf
- The White House (2011b) *Unified Command Plan 2011*. Washington, DC: The White House, April 6.

3.11 Supranational initiatives

Following an additional request from CATS, we have included below case studies relating to the cyber-security approaches of two key supranational organisations: NATO and the EU. We anticipate that the drivers for their policy approaches relate to their organisational objectives of increasing coordination and interoperability between states (certainly the case for the EU as it does not 'own' its own cyber-defence infrastructure, but less so for NATO as it has possesses assets such as C4I[75] infrastructure, etc).

[75] Command, Control, Communications, Computers and Information.

3.12 North Atlantic Treaty Organization (NATO)

3.12.1 Summary

NATO has prioritised the cyber threat as an emerging and continuing transnational challenge, alongside other priority areas such as proliferation, terrorism, maritime and energy security. NATO characterises cyber threats as a supranational challenge, but provides no further detail on threat actors. In terms of response structures, NATO has set up the Cyber Defence Management Board and the NATO Computer Incident Response Capability.

3.12.2 Introduction

Cyber defence is a key component of NATO's strategic concept. Adopted at the 2010 Lisbon Summit, the strategic concept tasked the North Atlantic Council with developing a new policy on cyber-defence.

3.12.3 The prioritisation of cyber threats in NATO risk assessment

The Lisbon Summit Declaration identifies cyber-security as "an emerging and continuing, trans-national challenge" among a list of other priority areas that include "proliferation, terrorism, maritime and energy security".[76] The revised policy was approved by ministers on 8 June 2011, and currently the associated action plan is being implemented. The strategic concept provides a blueprint for combating attacks through centralisation of cyber-protection and better integration of cyber-awareness, warning and response from member nations.[77] Further, it sets standards for cyber-defence cooperation with partner countries, international organisations, the private sector and academia. Bulgaria, Estonia, Poland, Slovakia, Turkey, the UK and the USA have all signed agreements with NATO to facilitate cooperation in the event of a cyber-attack.[78] In addition, non-members are actively involved in NATO's cyber-security efforts: Ukraine, for example, is part of a working group with NATO on cyber and military reform.[79]

However, there are clear limits to NATO's influence over the cyber-systems of its 28 members, as each is responsible for its own cyber-security. With the exception of Albania, Belgium, Bulgaria, Czech Republic, Denmark, Greece, Hungary, Iceland, Italy, Latvia and Spain, most NATO countries have, or are developing, a cyber-security strategy. Although the majority of NATO nations agree that cyber-security is a matter of increasing concern, not all share the same threat perceptions or strategic priorities. These divergent strategies and approaches could limit the possible scope of NATO action. Furthermore, a NATO response – especially in the context of crisis management – is hampered by the strict mandate that it has regarding 'traditional' military roles outside of the extreme invocation of Article V of the NATO Charter. Put simply, NATO does not have the mandate to exercise authority or even provide soft guidance to civilian (non-military) or private sector infrastructures. This issue is especially important, given the multidisciplinary nature of

[76] NATO (2010).

[77] NATO (2010).

[78] Hunker (2010).

[79] Grauman (2012).

cyberspace, and the way in which cyber-defence crosses the boundaries of the public and private sectors.

3.12.4 How is the threat characterised?

Dramatic change in the cyber-landscape has prompted a shift in NATO threat perception and prioritisation. Although cyber-defence has been part of its political agenda since the 2002 Prague Summit, it was only after the 2007 Estonian cyber-attacks that NATO defence ministers called for the development of a NATO cyber-defence policy. Since 2007, cyber threats have multiplied and diversified, with the 2008 war in Georgia demonstrating the role of cyber-attacks in conventional warfare.[80] While efforts were concentrated primarily on protecting the communications systems owned and operated by the alliance prior to the 2007 and 2008 attacks, NATO's focus subsequently broadened to the cyber-security of individual allies. Alex Vandurme, Head of Engineering at the NATO Computer Incident Response Capability, considers Estonia and Georgia to be templates for future cyber-attacks: "The types of cyber-attacks experienced by Estonia and Georgia will become the most frequent form of cyber-attack in the future – a mixture of protest, or traditional war, and a cybernetic element."[81]

On a more general level, NATO cyber strategies are designed to respond to espionage, destruction, crime and the theft of military and industrial secrets.[82] Further, the strategic concept identifies a range of hostile parties, namely "foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups".[83] It could be expected that NATO has specifically identified threat actors in classified assessments, but we were unable to gain access to such documentation.

3.12.5 Entities involved in response

In response to the proliferation and diversification of threats, NATO has strengthened commitment to combating cyber-attacks. In February 2012, NATO awarded a €58m contract to a Grumman and Finmeccanica team to strengthen the NATO Computer Incident Response Capability. This is expected to be fully operational by the end of 2012.[84] Heightened commitment to cyber-defence is reflected also in the creation of the NATO Communications and Information Agency on 1 July 2012, and current efforts to set up a cyber-threat awareness cell.

Implementation of the action plan entails operationalisation of 'rapid reaction team' network defenders by the end of 2012. The rapid reaction team capability will consist of a permanent core of six specialised experts who can coordinate and execute team missions. These cyber-experts will be braced to deploy within 24 hours to any NATO nation facing substantial attacks on its IT infrastructure.[85] Rapid reaction team efforts will focus

[80] NATO (2012b).

[81] Seffers (2012)

[82] NATO (2012a).

[83] NATO (2010).

[84] Benitez (2012).

[85] Benitez (2012).

primarily on prevention and deterrence, and any NATO member nation under cyber-attack can request the team's assistance through the Cyber Defence Management Board.[86]

The Cyber Defence Management Board consists of NATO's political, military, operational and technical cyber leaders. Its purpose is to coordinate cyber-defence activities throughout NATO and associated agencies, and to facilitate implementation of NATO's cyber-defence policies and capabilities through signing memoranda of understanding with the appropriate national authorities.

The Cooperative Cyber Defence Centre of Excellence is also a key component of NATO's cyber-defence effort. The Centre was established in Tallinn, Estonia on 14 May 2008, and constitutes an international effort that currently includes Estonia, Germany, Hungary, Italy, Latvia, Lithuania, Poland, Slovakia, Spain, the Netherlands and the USA.[87] The primary purpose of the Centre is to improve cyber-defence interoperability within the NATO network-enabled capability environment; to enhance information security and cyber-defence education, awareness and training; and to analyse legal aspects of cyber-defence. The Centre conducts research and training on cyber-security, and employs a staff of approximately 30. Turkey has announced its intent to join in the near future, and NATO has shown interest in extending membership to Iceland.

Responsibility for implementing the revised NATO policy on cyber-defence lies with NATO's political, military and technical authorities and individual allies. The North Atlantic Council oversees the political aspects of implementation and exercises principal decision-making authority regarding cyber crisis management. The Defence Policy and Planning Committee convenes defence counsellors from all national delegations, appraising cyber-capabilities and planning processes.

3.13 The European Union

3.13.1 Summary

Currently, the extent to which the EU prioritises cyber-security threats against other threats (eg pandemics, terrorism) is not known or visible, but is understood to be high on the future policy agenda.

Europol has released a public version of its Internet Organised Crime Threat Assessment (iOCTA). Response at the policy level is across a number of institutions covering cybercrime, foreign and security policy and improving cyber-security in government and business. Within the EU institutions, CERT-EU has been recently established as a reactive incident response capability to support the work of other CERTs including the EU–Council Network Cyber Defence Capability.

3.13.2 Introduction

The EU has constructed a comprehensive approach to cyber-security and at present has no public overarching strategy, although it is known that a European Cyber Security Strategy

[86] Seffers (2012).

[87] The Co-operative Cyber Defence Centre of Excellence. As of 5 December 2012: http://www.ccdcoe.org/

is at an advanced state of preparation. The need to focus on a more holistic and coordinated approach has been highlighted in several European Commission communications,[88] and the Commission has taken some tangible steps towards creating a pan-European policy. Charged with leading that effort, the EU's High Representative Catherine Ashton, Home Affairs Commissioner Cecilia Malmström and Digital Agenda Commissioner Neelie Kroes are working on a comprehensive European Cyber Security Strategy across the main relevant policy domains: international strategy and defence policy with respect to cyber-security, tackling cybercrime and addressing the resilience of cyberspace.

3.13.3 The prioritisation of cyber threats in EU risk assessment

Currently, Neelie Kroes is formulating specific legislative guidance as part of an internet security strategy for Europe, within the European Commission Work Programme for 2012.[89] This work will be undertaken by the Directorate-General for Communications Networks, Content and Technology (DG CNCT)[90] and seeks to strengthen the resilience of critical infrastructure, enhance preparedness and foster a cyber-security culture through the centralisation of information, private sector partnerships, single market-based approaches and an international outlook.[91]

Further, the EU Internal Security Strategy in Action outlines five steps towards a more secure Europe,[92] setting cyber-security enhancement for citizens and business among its key objectives.[93] Another significant step has been the implementation of a Digital Agenda for Europe in 2010 by the European Commission, which includes 14 actions to improve Europe's capability to prevent, detect and respond to network and information security-related problems.[94] These actions range from creating a new cybercrime platform (as part of the proposed European Cybercrime Centre),[95] to awareness campaigns for the online safety of children.[96] In accordance with the agenda, a pre-configuration team for the first full-scale CERT for the EU institutions was established in June 2011. This is meant to supplement the work of a range of other incident response and mitigation capabilities across the EU, including within the Commission (DG DIGIT in Luxembourg); Council (GSC in Brussels) and in other agencies.[97] The GSC has reportedly developed core capabilities to protect both classified and unclassified networks. GSC is also building up a

[88] European Commission (2005) 717/2; European Commission (2006) 251; European Commission (2010).

[89] European Commission, COM (2011) 623.

[90] DG INFSO before July 2012.

[91] Ashford (2012); European Commission (2012b).

[92] European Commission, COM (2010) 673.

[93] See in particular Objective 3, European Commission, COM (2010) 673, pp. 9, 17.

[94] European Commission, COM (2010) 245.

[95] To be operationalised in March 2013.

[96] European Commission (2010).

[97] European Commission (2012a).

cyber threat intelligence analysis capability fed by multiple sources. It is planned to standardise and characterise threat information and relate it to other cyber information in order to perform risk management.

Transatlantic cooperation is another important pillar of EU cyber initiatives: the EU–US Summit of November 2010 established an EU–US Working Group on Cyber-security and Cyber-crime.[98] By contrast, there are constraints on EU–NATO cooperation in cyber threat analysis, as information exchange runs into the same familiar institutional obstacles as their cooperation in other areas (notably the Turkey–Cyprus issue). These obstacles are unlikely to be overcome in the near future.

As yet, there has been little visibility of efforts either to prioritise these risks in comparison to each other, or to place these risks alongside others (eg climate change, demographics, armed conflict, etc).[99] The EU's Intelligence Analysis Centre (EU-INTCEN) in the European External Action Service builds a threat intelligence picture via the contributions of Member States, and acts on behalf of Member States with respect to gaps in intelligence. It also provides analysis for EU institutions on threats to European security.[100]

3.13.4 How is the threat characterised

There is no one single EU-level assessment that uses an 'all hazards' approach. For example, as the EU's criminal intelligence organisation, Europol has released a public version of its iOCTA[101] however, this is not related to other types of threat. Unofficially, it is understood from the European External Action Service[102] that the following actor types are considered:

- states
- state-sponsored
- proxies (entities acting on behalf of states)
- organised crime
- nexus between organised crime–state-sponsored–independent groups
- non-state actors (protesters or hacktivists).

The Digital Agenda for Europe emphasises the increasingly interconnected nature of threats and impact in cyberspace, and advocates coordinated responses accordingly. It emphasises that cyber threats are neither EU-specific, nor can they be overcome by the EU alone; rather, they can emanate from and affect any part of the world. The 14 actions proposed in the Digital Agenda for Europe specify a number of threats, including terrorist

[98] European Commission (2010).

[99] An assessment of global risks by the World Economic Forum may be insightful here, as cyber-terrorism and the failure of large-scale infrastructures were ranked as significant by business leaders alongside others such as climate change and demographic risks.

[100] Anonymous personal communication, European External Action Service, 5 December 2012.

[101] Europol (2011).

[102] Anonymous personal communication, European External Action Service, 5 December 2012.

or politically motivated attacks against information systems which form part of the critical infrastructures of the EU and its Member States. Online identity theft and fraud (which often take the form of 'Trojan Horses' and botnets) are identified also as key problems. Often, these are financially motivated, but also can be used for political ends, as in the cases of the cyber-attacks targeting Estonia, Georgia and Lithuania.

Other policy documents discuss and characterise the threat from serious and organised forms of cybercrime (eg Europol's iOCTA), identity theft and other forms of misuse.

3.13.5 Entities involved in the response

At present there is no single organisation or authority that is responsible for all EU cyber security in a similar way to NATO, or with state-level comparators. There are three different initiatives based on the institutional mandates of the EU prior to the Lisbon Treaty: cyber-resilience and the digital internal market (DG CNCT), tackling cybercrime and justice and home affairs cooperation (DG HOME) ; and the European External Action Service role in international cyber-issues and common defence and security policy. It is understood that a number of inter-institutional coordinating mechanisms operate between organisations with different portfolios. Leadership is being driven by a forthcoming European Cyber Security Strategy, which will have an EU legislative measure proposed by the European Commission to tackle network and information systems security (see below).

The 28-nation EU has no single approach to cyber-security; generally, responsibilities for internal security remain the prerogative of national governments. At the EU level, different issues are treated by different organisations. At the policy or strategic level there is no single equivalent to either the UK's OCSIA or NATO's Cyber Defence Management Board to take a proactive view of risks. The European Commission, European Parliament, European Council, European Central Bank, European Court of Justice and 55 other EU institutions and bodies will shortly have an operational, inter-institutional Computer Emergency Response Team (CERT-EU).[103] The team will operate under the strategic oversight of a steering board.[104] At present, this CERT does not seek to coordinate other national and government CERTs;[105] its scope is limited to EU institutions, bodies and agencies. Its aim is to promote new systems and stimulate information exchange between the community of CERTs and IT security companies in the EU institutions, Member States and elsewhere.[106] Operational national CERTs with international visibility can join the informal European Government CERTs Group (ECG) that is developing cooperation on incident responses between Member States.

The European Commission and the European Network and Information Security Agency (ENISA) are the chief interlocutors for cyber policy in the civilian area, and work closely with European Member States, especially competent authorities concerning Critical

[103] European Commission (2012a).

[104] European Commission (2012a).

[105] There are 140 CERTs in the EU and 23 EU Member State, national governmental CERTs.

[106] Grauman (2012).

Information Infrastructure Protection (CIIP), cybercrime (high-tech crime units) and national and/or governmental CERTs.

Within the Commission, the three main bodies responsible for formulation of a response are as follows:

- Directorate-General Home Affairs which is aimed at developing a common EU approach and supporting and facilitating the fight against cybercrime;
- DG CNCT (formerly DG Information Society and Media) – which aims to support resilience, CIIP and IT security through improved practice in Member States;
- European External Action Service – which recently has acquired interest in the domain and is developing the EU's foreign policy concerning cyberspace and cyber-security.

In addition, policy-level work of the directorates-general is complemented by three organisations (in varying stages of maturity) that have a more operational flavour, or have a role to play as a switching centre for good practice between the Member States of the EU.

Created in 2004, ENISA acts as a centre of excellence for Member States and EU institutions on network and information security issues, and has established itself rapidly as an actor in the European cyber-security community. In 2009, ENISA published a 'Good Practice Guide on National Exercises', and since then has held many workshops across Europe to assist in the planning of national exercises.[107] ENISA is also working on guidance for national cyber-security strategies.[108] ENISA saw its mandate extended by the Council after overseeing the coordination of the first pan-European cyber-security exercises in November 2010, and in 2011 the EU ruled that Member States have to report incidents to ENISA on a yearly basis. ENISA also facilitated the second pan-European cyber exercise, which took place on 4 October 2012. As stated in the evaluative report of Cyber Europe 2010, the Digital Agenda and the Commission Communication on Critical Information Infrastructure Protection, cyber exercises are an important element of a coherent strategy for cyber-incident contingency planning and recovery, both at the national and European levels. However, with a staff of 65, ENISA has an exceptionally small number of people relative to the breadth of its programmes and responsibilities.[109]

In March 2012, the European Commission announced its intent to set up a European Cybercrime Centre to be operational by the end of 2013 within Europol, the EU's criminal intelligence organisation. It will be based at Europol's headquarters in The Hague, and tasked with the coordination of national cybercrime authorities and training national experts.[110]

Finally, the European Defence Agency has been charged with the development of cyber-defence capability under the Capability Development Plan (CDP) agreed by the

[107] ENISA (2012b).

[108] For an initial overview, see ENISA (2012a).

[109] EuroWire (2011).

[110] Robinson (2012).

participating Member States in 2010. The European Defence Agency was set up in 2004; in the last three years it has begun to consider cyber-security and cyber-defence aspects from the perspective of the participating Member States. Currently, the Agency is completing a 'stocktaking' exercise on the cyber-defence capabilities of participating Member States, as well as considering opportunities for further work (such as the formulation of an EU military cyber-defence concept and a military cyber-defence centre).

3.14 Synthesis

This chapter has considered how official and grey policy documents reflect upon the priority that cyber-security threats are accorded in national risk assessment, the characterisation of those threats, and what can be determined as the lead responding authority.

Concerning the first question, we find from the comparators – where there is enough information available – that cyber-security threats appear to be characterised as high, major, prominent or priority when compared to other national level risks (for example, terrorism, pandemics, natural disasters, state-on-state conflict and nuclear war). We also encountered diversity in threat actor models, although some countries (Canada, Denmark, the Netherlands, the UK and the USA) referenced similar types of threat actor (organised crime, states and terrorist networks). Some countries (eg Germany, the Netherlands) also talk about threats which do not have an adversary, such as acts of nature and hardware and software failure.

Concerning the lead responding authority, again it was clear that different countries took different approaches. The UK (and to an extent, Canada) had a coordinating body. Some countries had set up or assigned specific departments or ministries (for example, the Estonian Authority for Information Systems, Dutch National Cyber Security Centre, French ANSSI and NATO's Cyber Defence Management Board. Finland had a highly distributed model, while Denmark has set up an approach where the Danish Security and Intelligence Service takes a lead, but with other departments assigned sectoral responsibility. The EU has a much more complex arrangement with separated mandates, suggesting a need for greater coordination and no single authority with responsibility.

Table 4 below summarises the analysis.

Table 4: Summary of the analysis

Comparator		What is the priority of cyber-security threats?	How is it defined/characterised?	What/who are the lead responding authorities?
1	Canada	One of seven highest	States (military and espionage) Cybercriminals Terrorist groups	Coordinating team within Public Safety Canada

2	Denmark	Highly likely	Financial damage Disruption or control of IT infrastructure and electronic warfare Espionage Cyber-relevance of terrorist threats	Sector responsibility, but leadership through the Danish Security and Intelligence Service and the National High Tech Crime Centre
3	Estonia	High (4 on a 5x5 matrix of impact and likelihood)	Focus on effects of threat actors	Estonian Authority for Information Systems
4	Finland	–	No typology available	Distributed among government departments
5	France	Major threat	No typology publicly used	Prime ministerial-level organisation (ANSSI)
6	Germany	–	Terrorism, crime and war Natural hazards and technical failure/human error	Federal Ministry of the Interior and National Cyber Defence Centre (NCAZ)
7	Netherlands	High priority	States Private organisations Professional criminals Terrorists Hacktivists Script kiddies Cyber-researchers Internal actors Non-actor	National Cyber Security Centre
8	Russian Federation	Most prominent(*)	Internal (crime and corruption) External (state, terrorists, foreign competition)	Security Council of the Federation/Ministry of Defence National system of information protection and intelligence community
9	United Kingdom	Tier 1 (highest level)	Criminals Nation-states Patriotic hackers Terrorist groups Hacktivists	Cabinet-level entity: Office for Cyber Security and Information Assurance
10	United States of America	Priority (one of four)	Criminal hackers Organised criminal groups Terrorist networks Advanced nation-states	Distributed across a number of organisations with Inter-agency Policy Committee
11	NATO	Priority challenge (alongside four others)	None publicly available	Cyber Defence Management Board NATO's Computer Incident Response Capability
12	EU	–	None available	Separate institutional mandates across protection of infrastructure of the EU (CERT-EU) Policy to tackle cybercrime (DG HOME/Europol) International security and defence (European External Action Service/European Defence Agency) and business/government security (DG CNCT/ENISA)

CHAPTER 4. Themes from the roundtable

Following data collection, analysis and circulation of the interim findings in October 2012, the analysis was presented at a half-day roundtable at CATS on 18 November 2012. The roundtable participants from CATS included a senior advisor on cyber security, the head of the cyber security unit, two representatives from the Swedish armed forces and a legal adviser. The study team leader and two analysts from RAND Europe attended. A presentation of the findings was used as a platform for broader discussion about a range of relevant topics to cyber-security.

The key themes for discussion arose from analysis of the case studies, but also RAND Europe's expert knowledge of the policymaking debate.[111] The aim of the roundtable was to provide some further insights and challenge to CATS in development of its national cyber security strategy, using the report as a starting point. This chapter is a record of the key themes discussed.

4.1 Themes from the findings

In terms of findings from the report, out of the 12 comparators where we had data, in some of the comparators that were studied (the Netherlands, the UK and the USA) cyber-security threats were described differently, but all use some kind of term synonymous with 'high'. Some countries (Estonia, the Netherlands and the UK) have applied quantitative estimates, as Table 5 shows.

Table 5: Prioritisation of cyber-security threats

	Comparator	Data available on priority?	Priority accorded?
1	Canada	Y	One of seven highest
2	Denmark	Y	Highly likely
3	Estonia	Y	High (4 on a 5x5 matrix of impact and likelihood)
4	Finland	N	–
5	France	Y	Major threat

[111] For example, the study team leader holds 'observer' status on the European Public Private Partnership for Resilience (EP3R): (http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.htm) and the Task Force on Incident Response as well as speaking in many conferences, eg the Cybersecurity Gathering (22 October 2012, Brussels): http://cybersecuritybrussels2012.eventbrite.com/

6	Germany	N	–
7	Netherlands	Y	High priority
8	Russian Federation	N	Most prominent(*)
9	UK	Y	Tier 1 (highest level)
10	USA		Priority (one of four)
11	NATO	Y	Priority challenge (alongside four others)
12	EU	N	–

(*) within the context of a subordinate strategy, the Critical Information Infrastructure Protection (CIIP) strategy

Of those countries for which information was available, the strategic and policy documents reviewed indicate that popular characterisations of cyber threats as either state-sponsored intelligence agencies, nation-states (as a supplementary activity or as part of hostile state-on-state conflict), serious and organised criminality and ideological threats. A good example in this regard is Estonia.

Our analysis of available strategic and policy documents indicates a tendency for strategies to reference some specific events (eg the Stuxnet malicious code, the distributed denial of service attacks in Estonia in 2007 or the Hackivist group 'Anonymous') as the rationale to capture the attention of policymakers. While it is important to capture policymakers' attention to support investment in cyber-security, we assert that the risk is that by focusing on a small number of well-known events, the capacity to deal with 'Black Swans'[112] – unexpected events – is undermined.

It is possible to ascertain that some uncertainty exists about terminology. In some cases what is identified as a threat is more properly a risk (ie a product of the probability of a threat actor exploiting vulnerabilities to create an impact). For example, in Estonia the threat is published as having been assessed according to the criteria used to assess risk (properly, a product of threat *x* vulnerability *x* impact). The Netherlands' Cyber Security Assessment 2012 discusses hardware or software failure leading to disruption of business services. This should be identified more properly not as a threat, but as impacts (disruption) resulting from vulnerabilities (failure in hardware or software). Finally, the Finnish National Security Strategy defines 'serious disruptions' as a threat scenario, but disruptions are actually the impacts or consequences of a threat exploiting vulnerabilities to achieve an impact.

Another preliminary conclusion is in how the response has been formulated. Sometimes cybercrime units are seen as playing an important role: this is the case for the National Bureau of Investigations in Finland, the Serious Organised Crime Agency in the UK; the IT Crimes Office of the Criminal Police in Estonia and within European structures, Europol. They collaborate with national or governmental Computer Emergency Response Teams (CERTs) eg in the UK and within the NATO Computer Incident Response Capability.

4.2 Shifting models of what constitutes cyber-security

It would appear that there is a shift in the terms of the debate in cyber-security, away from protection of information infrastructures and to protecting, as one recent Canadian

[112] Taleb (2010).

Security and Intelligence Service report puts it "the information based society as a whole".[113]

This report notes that existing, ad hoc and often uncoordinated defensive measures (for example, reactive incident response capabilities) on their own may not be sufficient to ensure the integrity and availability of information systems and critical infrastructure that support everyday life. Instead, cross-government and cross-sector nationally coordinated efforts may be required. These efforts should be based on a more proactive approach that is focused on prevention rather than reaction, and supported by intelligence capabilities that identify and prevent prospective attacks.[114]

In discussions at the EU policy level in Brussels and other national capitals (eg London and Washington, DC), policymakers' aims are becoming more strategic and include ensuring: that the cost to adversaries of trying to exploit systemic vulnerabilities is high (eg by implicitly trying to make it difficult to succeed in attacking the most attractive targets); that prospects for success are minimal, and that business and society are properly prepared and resilient. This is driving a more overt posturing of deterrence,[115] whereby some states (the Netherlands and the USA) make it clear that they are willing to undertake active measures in cyberspace, and are building 'offensive' capabilities often characterised as 'active defence' (eg the ability to break into computer networks of adversaries), which allow them to 'attack as the best form of defence'.[116] This may be regarded as a self-interested perspective, as states 'target harden' their own infrastructure, trying to alter the incentives for threat actors away from their own infrastructure.

4.3 Leveraging intelligence

Evidence from previous research into cybercrime units across Europe identifies that intelligence is a key component of tactical and strategic decision-making in this area to tackle cyber threats.[117] In the cyber domain, intelligence enhances governments' and stakeholders' ability to detect threats, assess the cyber-capabilities of adversaries, evaluate the effects of cyber-attacks and mitigate the risk. In turn, intelligence agencies are seeking (and securing) a larger role in the cyber-security domain across many the countries examined, reflected in the allocation of cyber-security programme budgets.[118]

---

[113] Gendron and Rudner (2012, p. 9).

[114] For example, the 'Four P's' approach of CONTEST, the UK's Counter-Terrorism strategy which seeks to Prevent, Protect, Prepare and Pursue terrorism (Home Office, 2012).

[115] Fryer-Biggs (2012).

[116] See, for example, the presentation by Henry (2012).

[117] Robinson et al. (2012) .

[118] For example, GCHQ received the lion's share of the UK's National Cyber Security Strategy budget (see also Bamford, 2012).

4.4 Understanding the purpose of the threat assessment

The discussion at the roundtable focused on the purpose of a cyber-security risk assessment. This must be carefully and clearly defined. Many of the policy documents identified in this study talk in broad terms about the threat from cyberspace – data loss, hackers or espionage and widespread criminal activities – for example, in the Estonian, German, UK and US case studies. Yet risk assessment relate fundamentally to the question of strategy (the definition of an active approach to tackling risks). Without a clear purpose to guide risk assessment – an understanding of 'what' you want to do once the threat has been identified – there is the opportunity for further uncertainty in how the results of a threat assessment can be used by responding authorities. In many cases, cyber-security strategies present lists of good practice or principles for governments to live by, rather than a strategy in the sense of a plan to pursue a defined goal.

To take a classical military example as a metaphor, a defence strategy might be defined along the lines of 'simultaneously fight and win two medium-sized conflicts while protecting the homeland'. Only when it has been determined who the threat actor is, and the likelihood of these conflicts occurring, will it be possible to develop a strategy (ie an active desire to do something) to mitigate the risk according to a set of principles (what the military might understand as doctrine, or what the private sector might understand as 'good practice').

4.5 What are the strategic assumptions about the threat?

One area in which there is scope for useful further analysis relates to the assumptions underlying each threat assessment: these are not openly described in the approaches of many countries covered in this study. One of the most important assumptions is how the threat is likely to evolve, based on either analysis of historical events or otherwise. Where there is an assumption that certain targets are attractive to a particular threat actor (for example, because of their wealth or for national security reasons), there should be consideration of how the attractiveness of these assets might evolve.

4.6 Public attribution of adversaries

The Netherlands' 2012 National Cyber Security Strategy and the US' recent attempt at articulating a Cybersecurity Act illustrate a belief that some cyber threat actors, namely foreign hostile states such as China, Iran and Russia, are more important to address than others (script kiddies, hacktivists). Public statements from officials are becoming increasingly open about identifying the sources of threat.[119]

4.7 A growing focus on public–private partnership

A growing area of emphasis for policymakers is combating digital espionage that targets not only government infrastructure, but also the intellectual property of businesses and

[119] Hague (2011).

highly relevant technology or innovation actors such as universities.[120] There would appear to be increasing consideration given to how to encourage the private sector to take such cyber national security issues seriously. Currently, the Canadian government is reviewing its strategy to generate ideas for better engagement with the private sector. Additionally, the UK government hopes to use eight universities, which are part of its Centres for Excellence in Cyber Security Research, to provide a foothold in the university realm.[121] Reaching beyond the inner circle of critical national infrastructure providers remains a challenge business sectors particularly sectors such as retail and engineering where cultures of cyber-security are less mature.[122]

There is debate in Europe about how to encourage the private sector to shoulder some responsibly for cyber-security. Many strategies reflect this kind of collaborative approach. There is little solid evidence on what this balance should be and, at the European level, how advice and support to EU Member States should be provided when there is such disparity and fragmentation in governmental approaches to regulation and the appetite for public–private partnership across the EU as a whole.

[120] Alperovich (2011).

[121] Engineering and Physical Sciences Research Council (2012).

[122] ENISA (2010a).

CHAPTER 5. Conclusions

This chapter presents some overall conclusions from the results of the study. This report has presented information derived from desktop research of policy documents and the grey literature to answer the following research questions.

- What level are cyber-security threats placed in relation to other national security threats?
- How are cyber threats characterised and defined?
- Who and what sort of national-level response mechanisms exist, and what role does law enforcement play in this?

In order to answer these questions publicly available documents concerning the 12 comparators were reviewed: ten countries and two supranational entities. This was accomplished by visiting the websites of government departments, ministries and other relevant public sector organisations, and downloading and reviewing published strategies and other policy documents. In addition, previous reports were reviewed to locate relevant documentation. In general, some publicly available information was found, with exceptions where strategies or risk assessments were not made public (eg France, Russia). Some countries (eg Estonia, the Netherlands and the UK) openly published more detail on how they had undertaken their assessments.

Table 6 summarises the findings across each of these research questions.

Table 6: Summary overview of results

Comparator	Level of prioritisation	Characterisation of threat	Lead responding authority
Canada	One of seven highest	States (military and espionage) Cybercriminals Terrorist groups	Coordinating team within Public Safety Canada
Denmark	Highly likely	Financial damage Disruption or control of IT infrastructure and electronic warfare Espionage Cyber-relevance of terrorist threats	Sector responsibility, but leadership through the Danish Security and Intelligence Service and the National High Tech Crime Centre
Estonia	High (4 on a 5x5 matrix of impact and likelihood)	Focus on effects of threat actors	Estonian Authority for Information Systems
Finland	–	No typology available	Distributed among government departments
France	Major threat	No typology publicly used	Prime Ministerial level organisation (ANSSI)
Germany	–	Terrorism, crime and war Natural hazards and technical failure and/or human error	Federal Ministry of the Interior and National Cyber Defence Centre (NCAZ).
Netherlands	High priority	States Private organisations Professional criminals Terrorists Hacktivists Script kiddies Cyber-researchers Internal actors Non-actor	National Cyber Security Centre
Russian Federation	Most prominent(*)	Internal (crime and corruption) External (state, terrorists, foreign competition)	Security Council of the Federation/ Ministry of Defence National system of information protection and intelligence community
UK	Tier 1 (highest level)	Criminals Nation-states Patriotic hackers Terrorist groups Hacktivists	Cabinet level entity: Office for Cyber Security and Information Assurance
USA	Priority (one of four)	Criminal hackers Organised criminal groups Terrorist networks Advanced nation-states	Distributed across a number of organisations with Inter-agency Policy Committee

NATO	Priority challenge (alongside four others)	None publicly available	Cyber Defence Management Board Cyber Defence Management Agency NATO's Computer Incident Response Capability Technical Centre
EU	–	None publicly available	Separate institutional mandates across protection of infrastructure of the EU (CERT-EU) Policy to tackle cybercrime (DG HOME/Europol) International security and defence (European External Action Service/ European Defence Agency) and business and/or government security (DG CNCT/ ENISA)

CHAPTER 6. Next steps

Noting the early stage of development of the cyber-security strategy in Sweden, we propose three broad themes for consideration, going forward. These aim to support the Swedish government in its preparations to develop its own cyber-security strategy, based on an assessment of the threats and risks.

6.1 The use of international comparisons

The research for this study has illustrated the sheer variety in how cyber threats are prioritised and defined, and how organisational responses are established across the different comparator states. The descriptions of the cyber-security postures of the case studies set out in Chapter 3 must be seen within the context of each country, and how relevant administrative structures are set up. For example, the extent to which a national-level command authority or a devolved approach is used is a product of institutional cultures and the way in which public administration is handled in each country, as well as legal and historical legacies. For example, neighbouring countries to Sweden applying a concept of 'total defence'[123] within their national security approach. This is different to the approach taken elsewhere, for example in France or the Netherlands. Understanding the institutional and strategic drivers informing these approaches helps to place lessons learned from elsewhere in context, and ensures that such lessons are applied appropriately.

6.2 Distinguish between risk and threats in national assessments

Estonia and Finland appear to define risks as threats. It is important to consider the basic definitions of risk as being a product of threat, vulnerability and consequence. The threat might be a nation-state (specifically attributed or not); vulnerabilities might be poor cyber-security training or a lack of skills within the technical community, resulting in poorly configured infrastructure. The impact might be micro- (losses to a firm) or macro- (effect upon gross domestic product, GDP) economic damage, loss of freedom of manoeuvre in cyberspace or national prestige.

[123] For example, see Foghelin (2009).

Being clear on the terminology helps to understand priorities, provide realistic appreciation of where resources ought to go, and the role that policy plays in building resilience to cope with a wide range of threats.

In addition, there is a related issue about the difference between threats and systemic risk. This is highlighted in assessments such as those from the Netherlands – which identify 'non-actor' threats – and Germany, where the threat from technical failure and natural disasters is identified. However, classically, threats are considered to be where there is a motivated adversary who exercises choice.[124] As a complex system with no single authority in control, cyberspace has chaotic properties that exhibit systemic risk: examples are 'route-flap', which occurs with misconfigured routers,[125] or an act of nature cutting submarine fibre-optic cables. The impacts of these accidents may be just as bad (if not worse) than those perpetrated by a strategic adversary. Indeed, the failure of submarine cables in the South China Sea in 2009[126] resulted in the loss of internet connectivity for some weeks, exceeding that of the Estonian distributed denial of service attacks.

Thus, any threat assessment should distinguish carefully strategic adversaries from systemic risk.

6.3 Take advantage of available multidisciplinary approaches to threat assessment

Finally, the Netherlands and the UK have openly published quantitative rankings of the assessments of cyber threats in comparison to other national-level threats. This moves away from a narrow approach to one where it is possible to understand these issues within the context of other national threats.

However, it might be possible to gain valuable insight and improved robustness of the assessments if they also have a quantitative character. Although care should be taken, it is important to take an approach that leverages the strength of different types of data in order to build a robust assessment. The use of quantitative approaches might help to place cyber-security threat assessments on a similar footing to those in other areas where more data exists (eg flood risk).

[124] Willis et al. (2005).

[125] ENISA (2010b).

[126] Carter et al. (2009).

REFERENCES

REFERENCES LIST

Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law (2011) "Cyber Warfare", No 77. The Hague AIV/No 22, CAVV December 2011.

Al Jazeera (2012) "Swedish government sites hit by cyber attacks", 3 September. As of 5 December 2012: http://www.aljazeera.com/news/europe/2012/09/201293182411421975.html

Alperovich, D. (2011) *Revealed: Operation Shady RAT*. As of 5 December 2012: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

Anderson, R., Barton, C., Boehme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T. and Savage, S. (2012) *Measuring the cost of cybercrime*. As of 5 December 2012: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Ashford, W. (2012) "EC opens cyber security consultation", *ComputerWeekly.com*. As of 5 December 2012: http://www.computerweekly.com/news/2240160072/EC-opens-cybersecurity-consultation

Ashford, W. (2012) "EU to set up cyber crime centre", *ComputerWeekly.com*, 27 March. As of 5 December 2012: http://www.computerweekly.com/news/2240147524/EU-to-set-up-cybercrime-centre

Bamford, J. (2012) "The NSA is building the country's biggest spy center (watch what you say)" *Wired*, 15 March. As of 5 December 2012: http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/

Benitez, J. (2012) "NATO's Cyber Rapid Reaction Team to be operational in 2012", *NATOSource Alliance News Blog*, 26 March. As of 5 December 2012: http://www.acus.org/natosource/natos-cyber-rapid-reaction-team-be-operational-2012

Black, D., Royal Canadian Mounted Police (2011) *The RCMP's perspective on a Canadian cybercrime strategy*. As of 5 December 2012: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/WS3_David_Black_CCFC.pdf

Bush, G. W. (2003) *Homeland security presidential directive 7: critical infrastructure identification, prioritization, and protection*, 17 December. As of 5 December 2012: http://www.dhs.gov/homeland-security-presidential-directive-7#top

Bush, G. W. (2008) *The comprehensive national cybersecurity initiative (CNCI)*, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23): Cyber Security and Monitoring

Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D. and Irvine N. (2009). *Submarine Cables and the Oceans: Connecting the World*, UNEP-WCMC Biodiversity Series No. 31, p. 40. As of 5 December 2012: http://www.iscpc.org/publications/ICPC-UNEP_Report.pdf

Commission of the European Communities (2005) "i2010 – A European Information Society for growth and employment", COM (2005) 717/2, 1 June. As of 5 December 2012: http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/ia/i2010extended_impact_assessment.pdf

Commission of the European Communities (2006) "A strategy for a Secure Information Society – Dialogue, partnership and empowerment", COM (2006) 251. As of 5 December 2012: http://ec.europa.eu/information_society/doc/com2006251.pdf

Author??? (2010) "Communication from the Commission to the European Parliament and Council: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", COM (2010) 673.

Author??? (2010) "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A digital agenda for Europe", COM (2010) 245.

Daniel, L. (2012) "Intelligence leaders urge congress to act on cyber laws", *American Forces Press Service*, 2 February. As of 5 December 2012: http://www.defense.gov/news/newsarticle.aspx?id=67035

Danish Defence Intelligence Service (2011) *DDIS intelligence risk assessment*. As of 5 December 2012: http://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/risikovurdering2011_EnglishVersion.pdf

Danish Government (2004) *Proclamation of the Danish Preparedness Act LBK No.137*. As of 5 December 2012: http://biblio.crn.ethz.ch/risk/index.php/publications/show/236

Danish Security and Intelligence Service, Centre for Terror Analysis (2012) *National threat assessment*. As of 5 December 2012: https://www.pet.dk/~/media/Engelsk/VTD%20NTV%20UK/NTVUK20120131pdf.ashx

Denmark, The Liberal Party, the Social Democratic Party, the Danish People's Party, the Socialist People's Party, the Conservative Party, the Radical Liberal Party, the Liberal Alliance Party (2009) *Danish defence agreement 2010–2014*. As of 5 December 2012: http://merln.ndu.edu/whitepapers/Denmark2010-2014English.pdf

DiploNews (2012) "The cyber-threat is promoted as governments must take it seriously", *DiploNews*, 27 July. As of 5 December 2012: http://www.diplonews.com/articles/2012/20120727_Cyberthreat.php

Donohue, B. (2011) "Biggest hack in Swedish history affects politicians, journalists among others", *The Kasperky Lab Security News Service*, 26 October. As of 5 December 2012: http://threatpost.com/en_us/blogs/biggest-hack-swedish-history-affects-politicians-journalists-among-others-102611

Donovan, K. M. (2011) "Expanding the Department of Defense's role in cyber civil support", 17 June. As of 5 December 2012: http://www.dtic.mil/dtic/tr/fulltext/u2/a545641.pdf

Dutch Government (2011) *The national cyber security strategy (NCSS): success through cooperation*. As of 5 December 2012: http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

Engineering and Physical Sciences Research Council (2012) "UK Universities awarded Academic Centre of Excellence for Cyber Security Research", 15 May. As at 5 December 2012: http://www.epsrc.ac.uk/newsevents/pubs/mags/connect/2012/86/Pages/ukuniversitiesawardedacademiccentreofexcellence.aspx

European Network and Information Security Agency (ENISA) (2010a) *Incentives and Challenges to Information Sharing*. As of 5 December 2012: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange

ENISA (2010b) *Inter-X: Resilience of the Internet Interconnection Ecosystem*. As of 5 December 2012: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx/inter-x

ENISA (2011a) *ENISA Country Reports: France Country Report*. As of 5 December 2012: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/France.pdf

ENISA (2011b) *ENISA Country Reports: Germany Country Report*. As of 5 December 2012: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Germany.pdf

ENISA (2012a) *National cyber security strategies: Setting the course for national efforts to strengthen security in cyberspace*. As of 5 December 2012: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

ENISA (2012b) *Cyber-Europe 2012*. As of 5 December 2012: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012

Estonia, Cyber Security Strategy Committee, Ministry of Defence (2008) *Cyber security strategy*. As of 5 December 2012: http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

Estonian Government (2010) *National security concept of Estonia*. As of 5 December 2012: http://www.mod.gov.ee/files/kmin/nodes/9470_National_Security_Concept_of_Estonia.pdf

Estonia, Ministry of the Interior (2011) *National emergency risk assessment*. As of 5 December 2012: https://www.siseministeerium.ee/public/HO_RA_2011nov.pdf

European External Action Service (2012) *Graphic representation*. As of 5 December 2012: http://eeas.europa.eu/background/docs/organisation_en.pdf

European Commission (2010) *Cyber security: secure networks*. As of 5 December 2012: https://ec.europa.eu/digital-agenda/en/cyber-security

European Commission (2011) COM 623 *Commission Work Programme.* As of 5 December 2012: http: //ec.europa.eu/atwork/programmes/docs/cwp2012_en.pdf

European Commission (2012a) "Cyber security strengthened at EU institutions following successful pilot scheme". As of 5 December 2012: http://europa.eu/rapid/press-release_IP-12-949_en.htm?locale=en

European Commission (2012b) *Proposal on a European strategy for internet security*. As of 5 December 2012: http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

Europol (2011) *Threat Assessment (Abridged): Internet Facilitated Organised Crime,* O2 – Analysis & Knowledge, File No. 2530-264, 7 January. As of 5 December 2012: https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf

EuroWire (2011) "The growing pains in EU cyber security policy". As of 5 December: http://www89.pair.com/bfemail/EuroWire-July2011.pdf

Faber, F. (2009) "Be ready – prepare together: workshop on the establishment of a European public–private partnership for resilience (EP3R)", 17 June, Brussels. As of 5 December 2012: http://ec.europa.eu/information_society/policy/nis/docs/ep3r_workshop/06_faber_nita_dk.pdf

Federal Bureau of Investigation (n.d.) Cyber crime: National Cyber Investigative Joint Task Force. As of 5 December 2012: http://www.fbi.gov/about-us/investigate/cyber/ncijtf

Finland, Ministry of Defence (2006) *Securely into the future: Ministry of Defence strategy 2025*. As of 5 December 2012: http://www.defmin.fi/files/674/Securely_into_the_future_-_strategy_2025.pdf

Finland, Ministry of Transport and Communications (2011) *Enhancing the usability and availability of information infrastructure essential for securing the vital functions of society: final report*. As of 5 December 2012: http://www.lvm.fi/c/document_library/get_file?folderId=1551284&name=DLFE-11788.pdf&title=Julkaisuja%203-2011

Finnish Government (2010) *Security in society*. As of 5 December 2012, http://www.yhteiskunnanturvallisuus.fi/en

Foghelin, J. (2009) "Defence transformation with frictions: the case of Sweden". Paper prepared for the NATO RTO organisation, Stockholm, Sweden.

Fox, B. (2012) "Parliament demands single EU voice on cyber-security" *EUObserver.com*, 13 June. As of 5 December 2012: http://euobserver.com/creative/116606

France, Committee on Foreign Affairs, Defence and Armed Forces of the Senate (2012) *Cyberdefence: a global issue, a national priority*. As of 5 December 2012: http://www.senat.fr/rap/r11-681/r11-6811.pdf

France, Présidence de la République (2008) *The French white paper on defence and national security*. As of 5 December 2012: http://www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf

Freeze, C. (2012) "Canada needs to take threat of Chinese cyberespionage more seriously: former top spy" *The Globe and Mail*, 9 October. As of 5 December 2012: http://www.theglobeandmail.com/news/politics/canada-needs-to-take-threat-of-chinese-cyberespionage-more-seriously-former-top-spy/article4598561/

Fryer-Biggs, Z. (2012) "US Military Goes on Cyber Offensive", *DefenseNews*, 24 March. As of 5 December 2012: http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive

Gendron, A and Rudner, M. (2012) "Assessing cyber threats to Canadian infrastructure". As of 5 December 2012: http://www.csis-scrs.gc.ca/pblctns/cdmctrch/CyberTrheats_AO_Booklet_ENG.pdf

Germany, Federal Ministry of the Interior (2009) *National strategy for critical infrastructure protection (CIP Strategy)*. As of 5 December 2012: http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

Germany, Federal Ministry of the Interior (2011) *Federal cyber security strategy for Germany*. As of 5 December 2012: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

Government of the Russian Federation (2000) *Information security doctrine of the Russian Federation*. As of 5 December 2012: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument

Government of the Russian Federation (2009) *Russia's national security strategy to 2020*. As of 5 December 2012: http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020

Government of the Russian Federation (2011) *Convention on international information security*. As of 5 December 2012: http://www.mid.ru/bdomp/ns-

osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument

Grauman, B. (2012) "Cyber-security: the vexed question of global rules: an independent report on cyber-preparedness around the world", *Security & Defence Agenda*. As of 5 December 2012: http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf

Hague, W. (2011) UK Foreign Secretary William Hague Speech to London Cyberspace Conference, QE2 Conference Centre, London, November.

Henry, S. (2012) "Changing the security paradigm: taking back your network and bringing pain to the adversary", presentation at Defcon 2012, Las Vegas, NV, July.

Hunker, J. (2010) "Cyber war and cyber power: issues for NATO doctrine", NATO Defense College. As of 5 December 2012: http://www.ndc.nato.int/download/downloads.php?icode=230

Khalilzad, Z.M., White, J.P. and Marshall, A. W. (eds) (1999) *Strategic appraisal: the changing role of information in warfare*. Santa Monica, CA: RAND Corporation.

Luiijf, H., Besseling, K., Spoelstra, M. and de Graaf, P. (2011) *Ten national cyber security strategies: a comparison, CRITIS 2011,* 6th International Conference on Critical information infrastructures Security.

McConnell, M. J. (2008) *Annual threat assessment of the Intelligence Community for the Senate Armed Services Committee*, 27 February 2008). As of 5 December 2012: http://www.armed-services.senate.gov/statemnt/2008/February/McConnell%2002-27-08.pdf

Marlow, I. (2012) "Nortel turned to RCMP about cyber hacking in 2004, ex-employee says", *The Globe and Mail,* 6 September. As of 5 December 2012: http://www.theglobeandmail.com/technology/tech-news/nortel-turned-to-rcmp-about-cyber-hacking-in-2004-ex-employee-says/article534295/

National Defence and the Canadian Forces (2012) *Communications Security Establishment Canada*. As of 5 December 2012: http://www.vcds-vcemd.forces.gc.ca/sites/page-eng.asp?page=10414

North Atlantic Treaty Organization (NATO) (2010) *Active engagement, modern defence: strategic concept for the defence and security of the members of the North Atlantic Treaty Organisation adopted by heads of state and government in Lisbon.* As of 5 December 2012: http://www.nato.int/cps/en/natolive/official_texts_68580.htm#cyber

NATO (2012a) "NATO Rapid Reaction Team to fight cyber attack", 13 March. As of 5 December 2012: http://www.nato.int/cps/en/SID-CE02A48A-209BF26A/natolive/news_85161.htm

NATO (2012b) *NATO and cyber defence*. As of 5 December 2012: http://www.nato.int/cps/en/SID-59DE606F-F1DB4932/natolive/topics_78170.htm?

Netherlands, Ministry of Security and Justice (2010) *National risk assessment 2010*. As of 5 December 2012: http://www.infosecisland.com/blogview/13379-Cyber-Conflict-in-Dutch-National-Risk-Assessment-of-2010.html

Netherlands, National Cyber Security Centre, Ministry of Security and Justice (2012) *Cyber security assessment Netherlands: CSBN-2*. As of 5 December 2012: https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/trend-reports/the-english-version-of-the-cyber-security-report-2012.html

O'Dwyer, G. (2011) 20 October 2011 "Finland to develop cyber-defence counter-punch". *DefenseNews*, 20 October. As of 5 December 2012: http://www.defensenews.com/article/20111020/DEFSECT04/110200306/Finland-Develop-Cyber-Defense-Counterpunch-

Office of the National Counterintelligence Executive (2011) *Foreign spies stealing US economic secrets in cyberspace: report to congress on foreign economic collection and industrial espionage, 2009–2011*. As of 5 December 2012: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Public Safety Canada, Government of Canada (2010) *Canada cyber security strategy: for a stronger and more prosperous Canada*. As of 5 December 2012: http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf

Rid, T. (2011) "Germany's cyber security strategy", *Kings College London*, 8 March. As of 5 December 2012: http://kingsofwar.org.uk/2011/03/germanys-cyber-security-strategy/

Robinson, N., Disley, E., Potoglou, D., Reding, A., May Culley, D., Penny, M., Botterman, M., Carpenter, G., Blackman, C. and Millard, J. (2012) *Feasibility study for a European cyber crime centre*. TR-1218-EC. Santa Monica, CA: RAND Corporation.

Security Council of the Russian Federation (2012), *The main directions of the state policy in the field of security control systems and industrial process critical infrastructure of the Russian Federation*, As of 5 December 2012 (in Russian original) : http://www.scrf.gov.ru/documents/6/113.html

Seffers, G. I. (2012) "Alliance to Deploy Cyber Rapid Reaction Team," *SignalOnline*, 1 September. As of 5 December 2012: https://www.afcea.org/content/?q=node/10094

Taleb N. N. (2010) *The Black Swan: The Impact of the Highly Improbable* (2nd edn). New York: Random House.

The Economist Intelligence Unit and Booz Allen Hamilton (2012) *Cyber power index*. As of 5 December 2012: http://www.cyberhub.com/CyberPowerIndex

Traynor, I. (2007) "Russia accused of unleashing cyberwar to disable Estonia", *The Guardian*, 17 May. As of 5 December 2012: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

UK Cabinet Office (2009) *Cyber security strategy of the United Kingdom: safety, security and resilience in cyberspace*. As of 5 December 2012: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

UK Cabinet Office (2010) *A strong Britain in an age of uncertainty: the national security strategy*. As of 5 December 2012: https://update.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf

UK Cabinet Office (2011) *The UK cyber security strategy: protecting and promoting the UK in a digital world*. As of 5 December 2012: http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

UK Cabinet Office (2012) *National risk register of civil emergencies*. As of 5 December 2012: http://www.cabinetoffice.gov.uk/sites/default/files/resources/CO_NationalRiskRegister_2012_acc.pdf

UK, HM Government (2010) *Securing Britain in an age of uncertainty: the strategic defence and security review*. As of 5 December 2012: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf

UK Home Office (2011a), *CONTEST: The United Kingdom's strategy for countering terrorism*. As of 22 October 2012: http://www.homeoffice.gov.uk/publications/counter-terrorism/counter-terrorism-strategy/strategy-contest?view=Binary

UK Intelligence and Security Committee (2011) *Annual report 2010–2011*. As of 5 December 2012: http://www.official-documents.gov.uk/document/cm81/8114/8114.pdf

US Department of Homeland Security (2011) *The strategic national risk assessment in support of PPD 8: a comprehensive risk-based approach toward a secure and resilient nation*. As of 5 December 2012: http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf

US Federal Bureau of Investigation (2012) *National Cyber Investigative Joint Task Force*. As of 5th December 2012 at: http://www.fbi.gov/about-us/investigate/cyber/ncijtf

US, The White House (2003) *The national strategy to secure cyberspace*. As of 5 December 2012: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

US, The White House (2009) *Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure*. As of 5 December 2012: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

US, The White House (2010) *National security strategy*. As of 5 December 2012: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

US, The White House (2011a) *International strategy for cyberspace: prosperity, security, and openness in a networked world*. As of 5 December 2012: http://info.publicintelligence.net/WH-InternationalCyberspace.pdf

The White House (2011b) *Unified Command Plan 2011*. Washington, DC: The White House, April 6.

Volker-Wetzler LTC (n.d.) *Cyber defence organisation. Germany and the Bundeswehr*. As of 5 December 2012: http://www.comm.rtaf.mi.th/Sitedirectory/124/3146/3146_2_4-Volker-Wetzler.pdf

Wallinn, S. (2012) "Finland aims to become a global forerunner in cyber-security by 2016", *Vu d'Europe*, Spring. As of 5 December 2012: http://www.europesworld.org/NewFrancais/Accueil/Article/tabid/190/ArticleType/ArticleView/ArticleID/21935/language/fr-FR/Finlandaimstobecomeaglobalforerunnerincybersecurityby2016.aspx

Willis, H. H., Morral, A. R., Kelly, T. K. and Medby, J. (2005) *Estimating Terrorism Risk*. Santa Monica, CA: RAND Corporation. As of 5 December 2012: http://www.rand.org/pubs/monographs/MG388.html

Annex A: Events of national interest

Example case	Type	Motive	Threat actor	Threat vector	Victims	Impact
Morris worm (1980)	Worm	Curiosity	Individual	Virus	University computer systems	Negligible
Conficker (2008)	Botnet	Uncertain (could be used as a platform for fraud or theft but also disruption and destabilising internet infrastructure)	Individual	Malicious code (worm) via vulnerability in Microsoft software	French navy, French and UK Ministry of Defence computers (Conficker-B)	15m computers infected
Maroochy Shire (2000)	Critical infrastructure (CI) attack	Vengeance	Disgruntled employee	Compromise of Supervisory Control and Data Acquisition	Local residents and users of water and sewerage supply	Physical contamination of water supply
War of web defacements	Web defacement	Vengeance	Non-state actors	Compromise of web servers	Various websites	Neglible – loss of reputation
Titan Rain (2003 onwards)	Espionage	Exfiltration of national security-sensitive data	State-sponsored/ intelligence agency	Network intrusion	US government	Unknown
Byzantine Hades Candor Anchor Foothold	Espionage	Exfiltration of national security-sensitive data	Alleged Chinese technical reconnaissance unit in Chengdu	Spear-phishing using email	US military, governmental and private sector	?

Night Dragon	Intellectual Property (IP) espionage	Exfiltration of commercially sensitive information	Alleged China	Blended threat (social engineering, spear-phishing and remote access tools)	Energy and petrochemical companies	?
US Central Command (2008) Buckshot Yankee	Espionage	Exfiltration of national security information	Unknown	Infected flash drive	US Centcom and Department of Defense classified and unclassified systems	?
Aurora (2009)	IP espionage	Exfiltration of commercially sensitive information	China	Blended threat (malicious code, network intrusion)	34 firms in the defence, high-tech and financial sectors	?
Shady RAT (2006 onwards)	IP espionage	Exfiltration of commercially sensitive information	Alleged China	Remote access tool/Trojan horse	72 high-profile companies, UN,	?
RSA SecurID (2011)	Exfiltration of commercially and security sensitive information	Foreign policy/national security	China	Blended threat (spear-phishing, Microsoft Excel vulnerability)	Lockheed Martin, possible other defence contractors	?
Ghost RAT GhostNet (2009 onwards)	Espionage	Foreign policy/ national security	Nation-state (People's Republic of China)	Remote access tool/Trojan horse	Embassies, foreign ministries, ASEAN headquarters	?
Estonia (2007)	Attack against Critical Information Infrastructure	Foreign policy/ national security	State-sponsored proxies	Distributed denial of service	Transactional and informational services of Estonian public bodies	Outage in terms of days, Estonia temporarily cut off from internet
Georgia (2009)	Attack against Critical Information Infrastructure	Foreign policy/ national security	State-sponsored proxies	Distributed denial of service	Georgian government public bodies	Temporary loss of ability of Georgian government to communicate with outside world
Stuxnet (2009)	Sabotage	Foreign policy/ national security	Nation-state?	Malicious code	Nuclear control systems in specific facility	Disruption of specific CI in single facility
European Commission and European External Action Service (2011)	Espionage	Foreign policy	Nation-state?	Malicious code via email attachments (as with attacks against French Finance Ministry)	European Commission and European External Action Service	?

French Finance Ministry (2011)	Espionage	Foreign policy/ national security	Nation-state?	Malicious code via email attachments	French Finance Ministry	?
Anonymous (2011)	Activism	Protest	Activists (anonymous)	Distributed denial of service attacks Network intrusion	Various high-profile organisations in the public and private sectors	Loss of reputation and humiliation
Lulzsec (2011)	Activism	Protest	Activists (anonymous)	Distributed denial of service attacks Network intrusion	Various high-profile organisations in the public and private sectors	Loss of reputation and humiliation
Stratfor (2012)	Activism	Protest	Activists (anonymous)	Network intrusion	Stratfor (US website)	User profiles published
EU Emissions Trading System (2011)	Fraud	Economic gain	?	Account compromise	Estonian, Austrian, Czech, Polish and French carbon trading registries	Estimated US$38m stolen

Annex B: Table of national comparators

Country	The prioritisation of cyber threats in national risk assessment	Characterisation of the threat	Responsible governmental entity
Canada	National Cyber Security Strategy	• Military and intelligence organisations undertaking state-sponsored cyber-military and espionage activities (political, economic, commercial and military purposes) • cybercriminals (identity theft, money laundering, extortion) • terrorist groups (recruitment, fundraising, propaganda, attacks)	• Canadian Cyber Incident Response Centre within the Department of Public Safety – monitors threats, public safety and awareness • Communications Security Establishment Canada (independent agency, under Ministry of Defense) – detects and discovers threats, provides intelligence and cyber-security, responds to threats against government systems • Canadian Security Intelligence Service – investigates and analyses domestic and international threats to the security of Canada

Country	The prioritisation of cyber threats in national risk assessment	Characterisation of the threat	Responsible governmental entity
			• Royal Canadian Mounted Police (Integrated Cyber Crime Fusion Centre) – investigates suspected domestic and international criminal acts in cyberspace • Canadian networks and critical information infrastructure • Treasury Board Secretariat – responsible for the government's information security • The military (Department of National Defence and the Canadian Forces) – responsible for defending their own network
Denmark	Danish Defence Intelligence Service, Intelligence Risk Assessment 2011 Threat assessment of the Centre for Terror Analysis, Danish Security and Intelligence Service 2012	In Danish Defence Intelligence Service Risk Assessment, cyber is linked to overall threat. Cybercrime is a part of: • international terrorism • terrorist action against authorities, critical infrastructure assets, employees, the wider population, etc Centre for Terror Analysis: • Islamist terrorism • extremism • espionage	• Territorially responsible municipalities and sectorally responsible ministries; • Military • Law enforcement – national Danish police (Danish Security and Intelligence Service and National High Tech Crime Centre)

Country	The prioritisation of cyber threats in national risk assessment	Characterisation of the threat	Responsible governmental entity
Estonia	National Security Concept includes 2011 update of national emergency risk assessment National Cyber Strategy rates likelihood of cyber-attack as "high" (4D on a 5x5-scale assessment), 1–5 on likelihood and 1–5 on seriousness of impact	Cyber Security Strategy 2008–2013 rejects cyber-warfare, cybercrime cyberterrorism division: • cyber-attack against critical information infrastructure • cybercrime	• Estonian Authority for Information Systems (RIA)– coordinates government bodies for crisis management • Department of Critical Information Infrastructure Protection • Ministry of Interior, within which sits the IT Crimes Office of the Criminal Police • The military – has a crucial role in cyber-defence, particularly regarding its close cooperation with NATO through the Co-operative Cyber Defence Centre of Excellence, established in Tallinn
Finland	The Finnish National Cyber Security Strategy is in preparation Finnish national Strategy for Security in Society The strategy of the Finnish armed forces to 2025 Threat assessment of the Ministry for Transport and Communications	Conflation of cyber-related threats and risks. Includes terrorist groups, states and individual criminals as well as natural forces): • terrorist attack • criminal acts that endanger the population • criminal acts that endanger functions in society • information operation • armed incident • surprise military attack • large-scale incident • effects – disruption of electricity, telecommunications and TV/radio broadcasts, damage to ICT infrastructure • disruption of delivery of consumer goods and water, failure of payments, flooding	• Ministry of Defence specialised cyber warfare unit • Ministry of Finance • Ministry of Transport and Communications • Ministry of the Interior • Law enforcement – Cybercrime Investigations Unit within the National Bureau of Investigations

Country	The prioritisation of cyber threats in national risk assessment	Characterisation of the threat	Responsible governmental entity
France	White Paper on Defence and National Security (2008)	• states – espionage (military and industrial) • terrorist groups (dissemination of ideas and attacks)	• ANSSI (umbrella organisation under the prime minister, State Secretary of Defense and National Security Council), but certain responsibilities are left with other actors • Secretary General for Defence and National Security • Ministry of Defence • Direction Générale de l'Armement • Direction et Protection de la Securité de la Défense • Ministry of the Interior • Direction Centrale du Renseignement Intériur • Central Office for the Fight Against Crime Linked to Information,Technology and Communication • Gendarmerie National (special services for Judicial Research and Documentation and Electronic Criminal Research Institute)
Germany	Federal Cyber Security Strategy for Germany 2009 National Security for Critical Infrastructure Protection strategy	Threats from within and outside Germany: • international terrorism • sabotage • espionage • war • military operations • other forms of criminal activity	• National Cyber Security Council • Federal Ministry of Interior (BMI) has ultimate responsibility over policy development and implementation. (Supervises the following: • Federal Office for Civil Protection and

Country	The prioritisation of cyber threats in national risk assessment	Characterisation of the threat	Responsible governmental entity
		intentional threats: • credit card fraud • botnets • electronic viruses • worms • Stuxnet-type attacks	Disaster Assistance • Federal Office for Information Security (BSI) • Federal Criminal Police Office • National Cyber Defence Centre (NCAZ), Centre – reports to the BSI and cooperates directly with the Federal Office for Civil Protection and Disaster Assistance and the Federal Office for the Protection of the Constitution, Federal Criminal Police Office, federal police, Customs Criminological Office, Federal Intelligence Service, Bundeswehr and authorities supervising critical infrastructure operators. All participate in this Centre within the framework of their statutory tasks and powers • Bundeswehr University: cyber-protection of the IT systems of the armed forces[127] • Information and Net operations section, CERT-Verbund
Netherlands	2010 National Risk Assessment	2012 Cyber Security Assessment	• National Cyber Security Centre (under the Ministry of Justice)

[127] Volker-Wetzler (n.d.).

Country	The prioritisation of cyber threats in national risk assessment	Characterisation of the threat	Responsible governmental entity
	2011 National Cyber Security Strategy (classifies cyber-security as a "high priority") 2012 Cyber Security Assessment	Actors: • states • private organisations • (professional) criminals • terrorists • hacktivists • script kiddies • cyber-researchers • internal actors • non-actor (natural or technological causes) Motivations: • states often target government bodies to improve their geopolitical position • private organisations attack their own competitors to advance their information position • professional criminals are driven by the promise of monetary gain • terrorists strive to secure ideological and political objectives • script kiddies are motivated by opportunism and the desire to experiment • cyber-researchers seek to profile themselves and expose weakness • internal actors act out of a sense of revenge,	• Dutch National High Tech Crime Unit within the Dutch National Police Agency • Dutch Electronic Crimes Task Force, National Police Services Agency, the National Public Prosecutor's Office (Landelijk Parket), banks and Dutch Centre for Protection of the National Infrastructure • Cyber Taskforce of the Ministry of Defence • General and military intelligence organisations (MIVD + AIVD)

Country	The prioritisation of cyber threats in national risk assessment	Characterisation of the threat	Responsible governmental entity
		carelessness or incompetence Resources: • states, private organisations and internal actors have the highest volume of resources • terrorists, hactivists and cyber-researchers perform the most visible attacks	
Russian Federation	Doctrine of Information Security National Security Strategy to 2020 National Security Strategy for Critical Infrastructure Protection Draft Convention on International Information Security to the UN	Doctrine of Information Security External threats: • attacks by foreign political, economic, military, intelligence and information entities • terrorist organisations • espionage with political, economic, industrial or military motivations • development by foreign states of definitions of cyberspace that infringe Russian sovereignty • foreign competition on the IT markets Internal threats: • organised crime infiltrating government systems • lack of adequate funding and governance structures • Corruption	• Security Council of the Federation, chaired by the President • Ministry of Defence – controls systems for certifying information protection tools (Federal Service for Technical and Export Control) • Ministry for Civil Defence – responsible for the national system of information protection • the intelligence community – including the Centre for Licensing, Certification and Protection of State Secrets of the Federal Security Service and the External Intelligence Service
UK	Cyber Security Strategy of The United Kingdom: safety,	National Risk Register: • cyber-attacks targeting infrastructure	• Office of Cyber Security and Information Assurance (OSCIA) – supports the

Country	The prioritisation of cyber threats in national risk assessment	Characterisation of the threat	Responsible governmental entity
	security and resilience in cyberspace 2009 The United Kingdom Cyber Security Strategy: protecting and promoting the UK in a digital world 2012 Strategic Defence and Security Review 2010 UK National Risk Register[128] – the non-classified version of the National Risk Assessment, performed yearly by the Cabinet Office characterises the cyber threat in the Tier 1 category (among the most prominent risks)	• cyber-attacks resulting in breach of data confidentiality Source of the threat: • states (economic, industrial and military espionage and disruption) • terrorist groups (propaganda, fundraising, planning) • politically active groups (disruption, profile-raising for hacktivists, reputational damage to target) Cyber-security strategy: • criminals • nation-states (intelligence and military operations) • economic, military or industrial espionage or disruption • patriotic hackers acting on states' behalf to spread misinformation • terrorist groups (propaganda and fundraising) • hacktivists (politically motivated groups) acting to cause reputational damage	Minister for the Cabinet Office and the National Security Council • Cyber Security Operations Centre – works with lead government departments and agencies (Home Office, Ministry of Defence, GCHQ, Communications Electronics Security Group, Centre for the Protection of National Infrastructure and Department for Business, Innovation and Skills) • Ofcom (communications regulator), • Information Commissioner's Office • Police departments – Serious Organized Crime Agency, the Police central e-crime Unit • Centre for the Protection of National Infrastructure – facilitates public–private partnership efforts in the UK • British intelligence community – has a particularly relevant role for GCHQ (hosts the Cabinet's Cyber Security

[128] Cabinet Office (2012).

Country	The prioritisation of cyber threats in national risk assessment	Characterisation of the threat	Responsible governmental entity
			Operations Centre) • Cybercrime unit for the upcoming National Crime Agency (previously handled by the Serious Organised Crime Agency; SOCA), to be set-up by 2013
			•
USA	Strategic National Risk Assessment in Support of PPD 8 2010 National Security Strategy: Cyber security one of four national security priorities 2011 US International Strategy for Cyberspace 2009 Cyberspace Policy Review 2008 Senate Armed Services Committee, Intelligence Community Annual Threat Assessment, February 2008	Strategic National Risk Assessment in Support of PPD 8[129] (unclassified summary) – cyber at top tier of threats. Not only considers cyber threats in isolation, but also notes the impact they have in shaping other threats. Cyber threats articulated at the top level of threat include: • cyber-attack against data (which seriously compromises the integrity or availability of data, ie the information contained in a computer system, or data processes resulting in economic losses of $1 billion or greater) • cyber-attack against physical infrastructure (ie used as a vector to achieve effects which are beyond the computer – kinetic or other effects – resulting in one fatality or greater or economic losses of $100m or greater)	Military and capabilities • Department of Defense • USNORTHCOM and USSTRATCOM Critical National Infrastructure: • Department of Homeland Security – is the National Cyber Security Center[130] • public–private partnerships on cyber-security, including the National Cyber Security Partnership Investigative and intelligence: • National Cyber Investigative Joint Task

[129] Department of Homeland Security (2011).

[130] System created by the National Strategy to Secure Cyberspace in 2003. It was further augmented later that year in Homeland Security Presidential Directive 7.

Country	The prioritisation of cyber threats in national risk assessment	Characterisation of the threat	Responsible governmental entity
		Senate Armed Services Committee, Intelligence Community Annual Threat Assessment, February 2008: • nation-states and criminals engaged in industrial espionage and terrorist organisations, including Al-Qaida, Hamas and Hezbollah 2010 National Security Strategy: • highlights the threat posed by criminal hackers • organised criminal groups • terrorist networks • advanced nation-states 2011 US International Strategy for Cyberspace: • actors characterising cybercriminals • states and their proxies	Force[131] – the FBI is responsible for developing and supporting the joint task force, which includes more than 20 intelligence agencies and law enforcement agencies Overall strategic direction: • 2012 Cyberspace Policy Review has tabled a set of actions for reviewing the cyber-defence system established by George W. Bush's 2008 Comprehensive National Cyber Security Initiative (more interagency coordination, counter-intelligence and awareness raising, among others), but the Senate has failed to reach an agreement over its implementation to date • The administration already has established an Information and Communications Infrastructure Interagency Policy Committee, chaired by the National Security Council and Homeland Security Council, as the primary policy coordination body for issues related to achieving an assured, reliable, secure and survivable global information and communications infrastructure

[131] Federal Bureau of Investigation (n.d.)